Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Notas y precauciones

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

PRECAUCIÓN: Un mensaje de PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos si no se siguen las instrucciones.

Marzo 2009 Rev. A00

Regresar a la página de contenido

Generalidades del subcomando RACADM

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

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

---

help

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

Tabla A-1. Comando help

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

Sinopsis

```
racadm help

racadm help <subcomando>
```

Descripción

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

Salida

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

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

Interfaces admitidas

- RACADM local

---

config

En la tabla A-2 se describen los subcomandos **config** y **getconfig**.

Tabla A-2. config/getconfig

Subcomando	Definición
config	Configura el iDRAC6.
getconfig	Obtiene los datos de configuración del iDRAC6.

Sinopsis

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

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

Interfaces admitidas

- RACADM local

Descripción

El subcomando **config** permite establecer los parámetros de configuración del iDRAC6 individualmente o procesarlos en lote como parte de un archivo de configuración. Si la información es diferente, el objeto iDRAC6 se escribe con los nuevos valores.

Entrada

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

Tabla A-3. Opciones y descripciones del subcomando config

Opción	Descripción
-f	La opción **-f** <*nombre_de_archivo*> permite que **config** lea el contenido del archivo especificado con el <*nombre_de_archivo*> y que configure el iDRAC6. El archivo debe contener los datos en el formato que se especifica en "Sintaxis del archivo de configuración" en la página 283.
-p	La opción **-p**, o de contraseña, indica a **config** que borre las anotaciones de contraseñas contenidas en el archivo config **-f** <*nombre de archivo*> después de que se completa la configuración.
-g	La opción **-g** <*nombre_de_grupo*>, o de grupo, se debe usar con la opción **-o**. El <*nombre_de_grupo*> especifica el grupo que contiene el objeto que se va a definir .
-o	La opción **-o** <*nombre_de_objeto*> <*valor*>, o de objeto, se debe usar con la opción **-g**. Esta opción especifica el nombre de objeto que se escribe con la cadena <*valor*>.
-i	La opción **-i** <*índice*>, o de índice, sólo es válida para grupos indexados y se puede usar para especificar un grupo exclusivo. El índice se especifica aquí mediante el valor del índice; no mediante un valor asignado.
-c	La opción **-c**, o de verificación, se usa con el subcomando **config** y permite analizar el archivo **.cfg** para encontrar errores de sintaxis. Si se encuentran errores, se mostrará el número de línea y una breve descripción de lo que está incorrecto. No se realizarán las operaciones de escritura en el iDRAC6. Esta opción es sólo una revisión.

Salida

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

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

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

Ejemplos

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

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

- `racadm config -f myrac.cfg`

  Configura o vuelve a configurar el iDRAC6. El archivo **myrac.cfg** se puede crear con el comando **getconfig**. El archivo **myrac.cfg** también se puede editar manualmente siempre y cuando se sigan las reglas de sintaxis.

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

---

getconfig

El subcomando **getconfig** permite recuperar los parámetros de configuración del iDRAC6 individualmente o se pueden recuperar todos los grupos de configuración del iDRAC6 y guardarse en un archivo.

Entrada

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

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

Tabla A-4. Opciones del subcomando getconfig

Opción	Descripción
-f	La opción **-f** <*nombre_de_archivo*> indica a **getconfig** que escriba toda la configuración del iDRAC6 en un archivo de configuración. Este archivo se puede usar entonces para realizar operaciones de configuración de procesamiento en lote por medio del subcomando **config**. **NOTA:** La opción **-f** no crea anotaciones para los grupos **cfgIpmiPet** y **cfgIpmiPef**. Usted debe establecer al menos un destino de captura para capturar el grupo **cfgIpmiPet** en el archivo.
-g	La opción **-g** <*nombre_de_grupo*>, o de grupo, se puede usar para mostrar la configuración de un solo grupo. El *nombre_de_grupo* es el nombre del grupo que se utiliza en los archivos **racadm.cfg**. Si el grupo es un grupo indexado, use la opción **-i**.
-h	La opción **-h**, o de ayuda, muestra una lista de todos los grupos de configuración disponibles que se pueden usar. Esta opción es útil cuando usted no recuerda los nombres exactos de los grupos.
-i	La opción **-i** <*índice*>, o de índice, sólo es válida para grupos indexados y se puede usar para especificar un grupo exclusivo. Si **-i** <*índice*> no se especifica, se asumirá un valor de 1 para los grupos, que son tablas que tienen varias anotaciones. El índice se especifica mediante el valor del índice; no mediante un valor asignado.
-o	La opción -o <*nombre_de_objeto*>, o de objeto, especifica el nombre de objeto que se usa en la consulta. Esta opción se puede usar con la opción **-g**.
-u	La opción **-u** <*nombre_de_usuario*>, o de nombre de usuario, se puede usar para mostrar la configuración del usuario especificado. La opción <***nombre_de_usuario***> es el nombre de usuario para inicio de sesión.
-v	La opción **-v**, o detallada, muestra detalles adicionales en propiedades y se utiliza con la opción **-g**.

Salida

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

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

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

Ejemplos

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig -f myrac.cfg`

  Guarda todos los objetos de configuración del grupo del iDRAC6 en **myrac.cfg**.

- `racadm getconfig -h`

  Muestra una lista de los grupos de configuración disponibles en el iDRAC6.

- `racadm getconfig -u root`

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

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

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

Sinopsis

```
racadm getconfig -f <nombre_de_archivo>

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

racadm getconfig -u <nombre_de_usuario>

racadm getconfig -h
```

Interfaces admitidas

- RACADM local

---

getssninfo

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

Tabla A-5. Subcomando getssninfo

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

Sinopsis

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

Descripción

El comando **getssninfo** muestra una lista de los usuarios que están conectados al iDRAC6. La información de resumen proporciona la siguiente información:

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

Interfaces admitidas

- RACADM local

Entrada

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

Tabla A-6. Opciones del subcomando getssninfo

Opción	Descripción
-A	La opción **-A** elimina la impresión de los encabezados de los datos.
-u	La opción de nombre de usuario **-u** <*nombre_de_usuario*> limita la salida impresa a sólo registros detallados de la sesión para el nombre de usuario

	determinado. Si se proporciona un asterisco (*) como nombre de usuario, aparecerá una lista de todos los usuarios. La información de resumen no aparecerá cuando se especifique esta opción.

Ejemplos

- `racadm getssninfo`

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

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

Usuario	Dirección IP	Tipo	Consolas
root	192.168.0.10	Telnet	KVM virtual

- `racadm getssninfo -A`

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

- `racadm getssninfo -A -u *`

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

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

---

getsysinfo

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

Tabla A-8. getsysinfo

Comando	Definición
getsysinfo	Muestra información del iDRAC6, información del sistema e información del estado de la vigilancia.

Sinopsis

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

Descripción

El subcomando **getsysinfo** muestra la información relacionada con el iDRAC6, el servidor administrado y la configuración de vigilancia.

Interfaces admitidas

- RACADM local

Entrada

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

Tabla A-9. Opciones del subcomando getsysinfo

Opción	Descripción
-d	Muestra la información del iDRAC6.

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

Salida

El subcomando **getsysinfo** muestra la información relacionada con el iDRAC6, el servidor administrado y la configuración de vigilancia.

Ejemplo del mensaje de salida

```
RAC Information:
RAC Date/Time            = Wed Aug 22 20:01:33 2007
Firmware Version         = 0.32
Firmware Build           = 13661
Last Firmware Update     = Mon Aug 20 08:09:36 2007

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

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

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

Ejemplos

```
racadm getsysinfo -A -s

"Información del sistema:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "Encendido"

racadm getsysinfo -w -s

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


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

Restricciones

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

---

getractime

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

Tabla A-10. getractime

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

Sinopsis

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

Descripción

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

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

Salida

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

Ejemplo del mensaje de salida

```
racadm getractime

Jue 8 de dic 20:15:26 2005

racadm getractime -d

20071208201542.000000
```

Interfaces admitidas

- RACADM local

---

setniccfg

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

Tabla A-11. setniccfg

Subcomando	Definición
setniccfg	Establece la configuración IP para el controlador.

Sinopsis

```
racadm setniccfg -d

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

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

Descripción

El subcomando **setniccfg** establece la dirección IP del iDRAC6.

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

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

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

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

Salida

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

Interfaces admitidas

- RACADM local

---

getniccfg

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

Tabla A-12. getniccfg

Subcomando	Definición
getniccfg	Muestra la configuración IP actual del iDRAC6.

Sinopsis

```
racadm getniccfg
```

Descripción

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

Ejemplo del mensaje de salida

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

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Interfaces admitidas

- RACADM local

---

getsvctag

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

Tabla A-13. getsvctag

Subcomando	Definición
getsvctag	Muestra la etiqueta de servicio.

Sinopsis

```
racadm getsvctag
```

Descripción

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

Ejemplo

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

```
Y76TP0G
```

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

Interfaces admitidas

- RACADM local

---

racreset

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

Tabla A-14. racreset

Subcomando	Definición
racreset	Restablece la configuración del iDRAC6.

NOTA: Cuando se ejecuta un subcomando racreset, es posible que el iDRAC6 tarde hasta un minuto para volver a un estado utilizable.

Sinopsis

```
racadm racreset
```

Descripción

El subcomando **racreset** realiza un restablecimiento del iDRAC6. El suceso de restablecimiento se escribe en el registro del iDRAC6.

Ejemplos

- `racadm racreset`

Iniciar la secuencia de restablecimiento mediante software del iDRAC6.

Interfaces admitidas

- RACADM local

---

racresetcfg

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

Tabla A-15. racresetcfg

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

Sinopsis

```
racadm racresetcfg
```

Interfaces admitidas

- RACADM local

Descripción

El comando **racresetcfg** elimina todas las anotaciones de la propiedad de base de datos configuradas por el usuario. La base de datos tiene propiedades predeterminadas para todas las anotaciones que se usan para restablecer los valores predeterminados originales del iDRAC6.

NOTA: Este comando elimina la configuración actual del iDRAC6 y restablece la configuración del iDRAC6 a los valores predeterminados. Después del restablecimiento, el nombre y la contraseña predeterminados son **root** y **calvin**, respectivamente, y la dirección IP es **192.168.0.120** más el número de la ranura en la que se encuentra el servidor en el chasis.

---

serveraction

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

Tabla A-16. serveraction

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

Sinopsis

```
racadm serveraction <acción>
```

Descripción

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

Tabla A-17. Opciones del subcomando serveraction

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

Salida

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

Interfaces admitidas

- RACADM local

---

getraclog

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

Tabla A-18. getraclog

Comando	Definición
getraclog -i	Muestra la cantidad de entradas del registro del iDRAC6.
getraclog	Muestra las anotaciones del registro del iDRAC6.

Sinopsis

```
racadm getraclog -i

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

Descripción

El comando **getraclog -i** muestra la cantidad de anotaciones en el registro del iDRAC6.

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

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

Tabla A-19. Opciones del subcomando getraclog

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

Salida

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

Ejemplo del mensaje de salida

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

Interfaces admitidas

- RACADM local

---

clrraclog

Sinopsis

```
racadm clrraclog
```

Descripción

El subcomando **clrraclog** elimina todas las anotaciones existentes del registro del iDRAC6. Se crea una nueva anotación para registrar la fecha y la hora en que el registro se borró.

---

getsel

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

Tabla A-20. getsel

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

Sinopsis

```
racadm getsel -i

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

Descripción

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

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

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

Tabla A-21. Opciones del subcomando getsel

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

Salida

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

Por ejemplo:

```
Record:      1
Date/Time:   16/11/05 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

Interfaces admitidas

- RACADM local

---

clrsel

Sinopsis

```
racadm clrsel
```

Descripción

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

Interfaces admitidas

- RACADM local

---

gettracelog

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

Tabla A-22. gettracelog

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

Sinopsis

```
racadm gettracelog -i

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

Descripción

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

Tabla A-23. Opciones del subcomando gettracelog

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

Salida

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

Por ejemplo:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

Interfaces admitidas

- RACADM local

---

sslcsrgen

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

Tabla A-24. sslcsrgen

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

Sinopsis

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

racadm sslcsrgen -s
```

Descripción

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

Opciones

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

Tabla A-25. Opciones del subcomando sslcsrgen

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

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

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

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

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

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

Ejemplos

```
racadm sslcsrgen -s
```

O bien:

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

Interfaces admitidas

- RACADM local

---

sslcertupload

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

Tabla A-26. sslcertupload

Subcomando	Descripción
sslcertupload	Carga un servidor SSL personalizado o un certificado de CA del cliente al iDRAC6.

Sinopsis

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

Opciones

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

Tabla A-27. Opciones del subcomando sslcertupload

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

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

Ejemplo

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

Interfaces admitidas

- RACADM local

---

sslcertdownload

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

Tabla A-28. sslcertdownload

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

Sinopsis

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

Opciones

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

Tabla A-29. Opciones del subcomando sslcertdownload

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

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

Ejemplo

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

Interfaces admitidas

- RACADM local

---

sslcertview

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

Tabla A-30. sslcertview

Subcomando	Descripción
sslcertview	Muestra el servidor SSL o el certificado de CA que existe en el iDRAC6.

Sinopsis

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

Opciones

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

Tabla A-31. Opciones del subcomando sslcertview

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

Ejemplo del mensaje de salida

```
racadm sslcertview -t 1

Serial Number             : 00

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

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

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

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
```

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

Interfaces admitidas

- RACADM local

---

testemail

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

Tabla A-32. Configuración de testemail

Subcomando	Descripción
testemail	Prueba la función de alertas por correo electrónico del iDRAC6.

Sinopsis

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

Descripción

Envía un correo electrónico de prueba del iDRAC6 a un destino especificado.

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

Tabla A-33. Configuración de testemail

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

Opciones

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

Tabla A-34. Opción del subcomando testemail

Opción	Descripción

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

Salida

Ninguna.

Interfaces admitidas

- RACADM local

---

testtrap

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

Tabla A-35. testtrap

Subcomando	Descripción
testtrap	Prueba la función de alertas de captura SNMP del iDRAC6.

Sinopsis

```
racadm testtrap -i <índice>
```

Descripción

El subcomando **testtrap** prueba la función de alertas de capturas SNMP del iDRAC6 mediante el envío de una captura de prueba del iDRAC6 a un receptor de capturas de destino especificado en la red.

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

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

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

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

Entrada

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

Tabla A-37. Opciones del subcomando testtrap

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

Interfaces admitidas

- RACADM local

---

vmdisconnect

Sinopsis

```
racadm vmdisconnect
```

Descripción

El subcomando **vmdisconnect** desconecta todas las conexiones de medios virtuales.

---

clrasrscreen

Sinopsis

```
racadm clrasrscreen
```

Descripción

Borrar la pantalla del último ASR (bloqueo)

---

localconredirdisable

Sinopsis

```
racadm localconredirdisable [0, 1]
```

Descripción

Desactivar kVM local del sistema local

Valores legales

`0` = Activar

`1` = Desactivar

---

vmkey

Sinopsis

```
racadm vmkey [ reset ]
```

Descripción

El subcomando **vmkey** restablece la memoria de medios virtuales al tamaño predeterminado de 256MB.

Valores legales

`reset` = restablece la memoria al tamaño predeterminado (256 MB)

---

version

Sinopsis

```
racadm version
```

Descripción

Mostrar la versión de RACADM

Regresar a la página de contenido

Regresar a la página de contenido

Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

La base de datos de propiedades del iDRAC6 contiene la información de configuración de éste. Los datos se organizan por objeto asociado y los objetos se organizan por grupos de objetos. Las identificaciones de los grupos y objetos admitidos por la base de datos de propiedades se enumeran en esta sección.

Use las identificaciones de objetos y grupos con la utilidad RACADM para configurar el iDRAC6. Las secciones siguientes describen cada objeto e indican si el objeto se puede leer, escribir o ambos.

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

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen el conjunto siguiente:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

Este grupo contiene parámetros de la pantalla para proporcionar información acerca de las características específicas del iDRAC6 que se está consultando.

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

idRacProductInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII

Predeterminado

Integrated Dell Remote Access Controller

Descripción

Una cadena de texto que identifica el producto

idRacDescriptionInfo (sólo lectura)

Valores legales

Cadena de hasta 255 caracteres ASCII

Predeterminado

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

Descripción

Una descripción de texto del tipo de RAC

idRacVersionInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII

Predeterminado

1

Descripción

Una cadena que contiene la versión actual del firmware del producto

idRacBuildInfo (sólo lectura)

Valores legales

Cadena de hasta 16 caracteres ASCII

Predeterminado

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

Descripción

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

idRacName (sólo lectura)

Valores legales

Cadena de hasta 15 caracteres ASCII

Predeterminado

iDRAC

Descripción

Un usuario asigna un nombre para identificar a este controlador

idRacType (sólo lectura)

Valores legales

Identificación del producto

Predeterminado

8

Descripción

Identifica el tipo de controlador de acceso remoto como el iDRAC6

---

cfgOobSnmp

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

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

cfgOobSnmpAgentCommunity (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 31

Predeterminado

público

Descripción

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

cfgOobSnmpAgentEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva el agente SNMP en el RAC

---

cfgLanNetworking

Este grupo contiene parámetros para configurar la NIC del iDRAC6.

Se permite una instancia del grupo. Todos los objetos en este grupo requerirán que se restablezca la NIC del iDRAC6, lo que puede ocasionar una breve pérdida de la conectividad. Los objetos que cambien la configuración de la dirección IP de la NIC del iDRAC6 cerrarán todas las sesiones de usuario activas y requerirán que los usuarios se vuelvan a conectar con la configuración actualizada de la dirección IP.

cfgDNSDomainNameFromDHCP (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Especifica que el nombre del dominio DNS del iDRAC6 se debe asignar desde el servidor DHCP de la red

cfgDNSDomainName (lectura/escritura)

Valores legales

Cadena de hasta 254 caracteres ASCII Al menos uno de los caracteres debe ser alfabético. Los caracteres se limitan a caracteres alfanuméricos, guiones y puntos.

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

Predeterminado

(vacío)

Descripción

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

cfgDNSRacName (lectura/escritura)

Valores legales

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

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

Predeterminado

idrac-*etiqueta de servicio*

Descripción

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

cfgDNSRegisterRac (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Registra el nombre del iDRAC6 en el servidor DNS

cfgDNSServersFromDHCP (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgDNSServer1 (lectura / escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

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

cfgDNSServer2 (lectura / escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

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

cfgNicEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva el controlador de interfaz de red del iDRAC6. Si la NIC está desactivada, las interfaces de red remotas al iDRAC6 ya no estarán accesibles y sólo se podrá acceder al iDRAC6 por medio de la interfaz de RACADM local.

cfgNicIpAddress (lectura/escritura)

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

Valores legales

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

Predeterminado

192.168.0.*n*

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

Descripción

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

cfgNicNetmask (lectura/escritura)

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

Valores legales

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

Predeterminado

255.255.255.0

Descripción

La máscara de subred que se utiliza para la asignación estática de la dirección IP del iDRAC6. Esta propiedad sólo es válida si **cfgNicUseDhcp** se establece como **0** (FALSE).

cfgNicGateway (lectura/escritura)

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

Valores legales

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

Predeterminado

192.168.0.1

Descripción

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

cfgNicUseDhcp (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Especifica si se utiliza DHCP para asignar la dirección IP del iDRAC6. Si esta propiedad se establece en 1 (TRUE), entonces la dirección IP del iDRAC6, la máscara de subred y la puerta de enlace se asignan a partir del servidor DHCP en la red. Si esta propiedad se establece como **0** (FALSE), la dirección IP, la máscara de subred y la puerta de enlace estáticas se asignarán a partir de las propiedades **cfgNicIpAddress**, **cfgNicNetmask** y **cfgNicGateway**.

cfgNicMacAddress (sólo lectura)

Valores legales

Una cadena que representa la dirección MAC de la NIC del RAC

Predeterminado

La dirección MAC actual de la NIC del iDRAC6. Por ejemplo, 00:12:67:52:51:A3.

Descripción

La dirección MAC de la NIC del iDRAC6

---

cfgUserAdmin

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

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

cfgUserAdminIndex (sólo lectura)

Valores legales

Este parámetro se debe establecer en función de las instancias existentes

Predeterminado

De 1 a 16

Descripción

Índice único de usuario

cfgUserAdminIpmiLanPrivilege (lectura/escritura)

Valores legales

2 (**Usuario**)

3 (Operador)

4 (**Administrador**)

15 (**Sin acceso**)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI

cfgUserAdminPrivilege (lectura/escritura)

Valores legales

0x00000000 a 0x000001ff y 0x0

Predeterminado

0x00000000

Descripción

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

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

Privilegio del usuario	Máscara de bits de privilegios
Iniciar sesión en el iDRAC6	0x0000001
Configurar el iDRAC6	0x0000002
Configurar usuarios	0x0000004
Borrar registros	0x0000008
Ejecutar comandos de control del servidor	0x0000010
Acceder a redirección de consola	0x0000020
Acceder a los medios virtuales	0x0000040
Probar alertas	0x0000080
Ejecutar comandos de depuración	0x0000100

Ejemplos

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

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

Privilegios del usuario	Máscara de bits de privilegios
El usuario no tiene permiso para acceder al iDRAC6.	0x00000000
El usuario sólo puede iniciar sesión en el iDRAC6 y ver la información de configuración del servidor y del iDRAC6.	0x00000001
El usuario puede iniciar sesión en el iDRAC6 y cambiar la configuración.	0x00000001 + 0x00000002 = 0x00000003
El usuario puede iniciar sesión en el RAC, acceder a los medios virtuales y acceder a la redirección de consola.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 16

Predeterminado

(vacío)

Descripción

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

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

cfgUserAdminPassword (de sólo escritura)

Valores legales

Una cadena de hasta 20 caracteres ASCII

Predeterminado

(vacío)

Descripción

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

cfgUserAdminEnable

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva un usuario individual

cfgUserAdminSolEnable

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

---

cfgEmailAlert

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

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

cfgEmailAlertIndex (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

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

Descripción

El índice único de una instancia de alerta

cfgEmailAlertEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgEmailAlertAddress

Valores legales

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

Predeterminado

(vacío)

Descripción

La dirección de correo electrónico del origen de la alerta

cfgEmailAlertCustomMsg

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Especifica el mensaje personalizado que se enviará con la alerta

---

cfgSessionManagement

Este grupo contiene parámetros para configurar la cantidad de sesiones que se pueden conectar al iDRAC6.

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

cfgSsnMgtConsRedirMaxSessions (lectura/escritura)

Valores legales

De 1 a 4

Predeterminado

4

Descripción

Especifica el máximo de sesiones de redirección de consola que se permiten en el iDRAC6

cfgSsnMgtWebserverTimeout (lectura/escritura)

Valores legales

De 60 a 10800

Predeterminado

1800

Descripción

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

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

cfgSsnMgtSshIdleTimeout (lectura/escritura)

Valores legales

0 (Sin tiempo de espera)

De 60 a 10800

Predeterminado

1800

Descripción

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

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

Warning: Session no longer valid, may have timed out
(Advertencia: La sesión ya no es válida, es posible que haya agotado el tiempo de espera)

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

cfgSsnMgtTelnetIdleTimeout (lectura/escritura)

Valores legales

0 (Sin tiempo de espera)

De 60 a 10800

Predeterminado

1800

Descripción

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

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

Warning: Session no longer valid, may have timed out
(Advertencia: La sesión ya no es válida, es posible que haya agotado el tiempo de espera)

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

---

cfgSerial

Este grupo contiene parámetros de configuración de los servicios del iDRAC6.

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

cfgSerialSshEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Activa o desactiva la interfaz de Secure Shell (SSH) en el iDRAC6

cfgSerialTelnetEnable (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de la consola Telnet en el iDRAC6

---

cfgRemoteHosts

Este grupo contiene propiedades que permiten la configuración del servidor de SMTP para las alertas de correo electrónico.

cfgRhostsSmtpServerIpAddr (lectura / escritura)

Valores legales

Una cadena que representa una dirección IP válida de servidor SMTP. Por ejemplo: 192.168.0.56.

Predeterminado

0.0.0.0

Descripción

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

---

cfgUserDomain

Este grupo se utiliza para configurar los nombres de dominio para los usuarios de Active Directory. Pueden configurarse hasta un máximo de 40 nombres de dominio por vez.

cfgUserDomainIndex (sólo lectura)

Valores legales

De 1 a 40

Predeterminado

<instance>

Descripción

Representa un dominio específico

cfgUserDomainName (lectura/escritura)

Valores legales

Una cadena de hasta 255 caracteres

Predeterminado

(vacío)

Descripción

Especifica el nombre de dominio de usuario de Active Directory

---

cfgServerPower

Este grupo proporciona varias funciones de administración de alimentación.

cfgServerPowerStatus (sólo lectura)

Valores legales

1 = TRUE

0 = FALSE

Predeterminado

0

Descripción

Representa el estado de la alimentación del servidor, ya sea **ENCENDIDO** o **APAGADO**

cfgServerPowerServerAllocation (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Representa el suministro de alimentación disponible para el uso del servidor

cfgServerPowerActualPowerConsumption (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Representa el consumo de alimentación del servidor actual

cfgServerPowerPeakPowerConsumption (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Representa el consumo máximo de alimentación del servidor hasta el momento

cfgServerPowerPeakPowerTimestamp (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Periodo en que se registró el consumo máximo de alimentación

cfgServerPowerConsumptionClear (sólo escritura)

Valores legales

0, 1

Predeterminado

0

Descripción

Restablece la propiedad **cfgServerPeakPowerConsumption** a 0 y la propiedad **cfgServerPeakPowerConsumptionTimestamp** a la hora actual del iDRAC6

cfgServerPowerCapWatts (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Representa el umbral de alimentación del servidor expresado en vatios

cfgServerPowerCapBtuhr (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Representa el umbral de alimentación del servidor expresado en BTU por hora

cfgServerPowerCapPercent (sólo lectura)

Valores legales

Una cadena de hasta 32 caracteres

Predeterminado

(vacío)

Descripción

Representa el umbral de alimentación del servidor expresado en porcentajes

---

cfgRacTuning

Este grupo se usa para establecer varias propiedades de configuración del iDRAC6, por ejemplo, las restricciones de puertos de seguridad y los puertos válidos.

cfgRacTuneHttpPort (lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

80

Descripción

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

cfgRacTuneHttpsPort (lectura/escritura)

Valores legales

De 10 a 65535

Predeterminado

443

Descripción

Especifica el número de puerto que se debe usar para la comunicación de red HTTPS con el iDRAC6

cfgRacTuneIpRangeEnable

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la función de validación de rango de dirección IP del iDRAC6

cfgRacTuneIpRangeAddr

Valores legales

Una cadena con formato de dirección IP. Por ejemplo, 192.168.0.44.

Predeterminado

192.168.1.1

Descripción

Especifica el patrón de bits de dirección IP aceptable en posiciones determinadas por los números 1 en la propiedad de máscara de rango (**cfgRacTuneIpRangeMask**)

cfgRacTuneIpRangeMask

Valores legales

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

Predeterminado

255.255.255.0

Descripción

Una cadena con formato de dirección IP. Por ejemplo, 255.255.255.0.

cfgRacTuneIpBlkEnable

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgRacTuneIpBlkFailCount

Valores legales

De 2 a 16

Predeterminado

5

Descripción

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

cfgRacTuneIpBlkFailWindow

Valores legales

De 10 a 65535

Predeterminado

60

Descripción

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

cfgRacTuneIpBlkPenaltyTime

Valores legales

De 10 a 65535

Predeterminado

300

Descripción

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

cfgRacTuneSshPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

22

Descripción

Especifica el número de puerto que se usa para la interfaz SSH del iDRAC6

cfgRacTuneConRedirEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Activa o desactiva la redirección de consola

cfgRacTuneTelnetPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

23

Descripción

Especifica el número de puerto que se usa para la interfaz Telnet del iDRAC6

cfgRacTuneConRedirEncryptEnable (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Cifra el vídeo en una sesión de redirección de consola

cfgRacTuneConRedirPort (lectura / escritura)

Valores legales

De 1 a 65535

Predeterminado

5900

Descripción

Especifica el puerto que se debe usar para tráfico de teclado y ratón durante la actividad de redirección de consola con el iDRAC6

cfgRacTuneConRedirVideoPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

5901

Descripción

Especifica el puerto que se debe usar para el tráfico de vídeo durante la actividad de redirección de consola con el iDRAC6

NOTA: Este objeto requiere de un restablecimiento de iDRAC6 antes de activarse.

cfgRacTuneAsrEnable (lectura/escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva la función de captura de pantallas de último bloqueo del iDRAC6

NOTA: Este objeto requiere de un restablecimiento de iDRAC6 antes de activarse.

cfgRacTuneWebserverEnable (lectura/escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa y desactiva el servidor web del iDRAC6. Si esta propiedad está desactivada, no se podrá tener acceso al iDRAC6 por medio de exploradores web clientes. Esta propiedad no tiene ningún efecto en las interfaces Telnet, SSH o RACADM local.

cfgRacTuneLocalServerVideo (lectura/escritura)

Valores legales

1 (activa)

0 (desactiva)

Predeterminado

1

Descripción

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

cfgRacTuneLocalConfigDisable (lectura/escritura)

Valores legales

0 (activa)

1 (desactiva)

Predeterminado

0

Descripción

Desactiva el acceso de escritura a los datos de configuración del iDRAC6. La opción predeterminada es el acceso activo.

NOTA: El acceso puede desactivarse utilizando la interfaz local RACADM o la interfaz web del iDRAC6; sin embargo, una vez desactivado, el acceso puede reactivarse solamente a través de la interfaz web del iDRAC6.

---

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres

Predeterminado

(vacío)

Descripción

El nombre de host del servidor administrado

ifcRacMnOsOsName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres

Predeterminado

(vacío)

Descripción

El nombre del sistema operativo del servidor administrado

---

cfgRacSecurity

Este grupo se usa para configurar los valores relacionados con la función de solicitud de firma de certificado (CSR) SSL del iDRAC6. Las propiedades en este grupo se deben configurar antes de generar una CSR a partir del iDRAC6.

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

cfgSecCsrCommonName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres

Predeterminado

Descripción

Especifica el nombre común (CN) de la CSR

cfgSecCsrOrganizationName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres

Predeterminado

(vacío)

Descripción

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

cfgSecCsrOrganizationUnit (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres

Predeterminado

(vacío)

Descripción

Especifica la unidad organizativa (OU) de la CSR

cfgSecCsrLocalityName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres

Predeterminado

(vacío)

Descripción

Especifica la localidad (L) de la CSR

cfgSecCsrStateName (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres

Predeterminado

(vacío)

Descripción

Especifica el nombre del estado (S) de la CSR

cfgSecCsrCountryCode (lectura/escritura)

Valores legales

Una cadena de dos caracteres

Predeterminado

(vacío)

Descripción

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

cfgSecCsrEmailAddr (lectura / escritura)

Valores legales

Una cadena de hasta 254 caracteres

Predeterminado

(vacío)

Descripción

Especifica la dirección de correo electrónico de CSR.

cfgSecCsrKeySize (lectura / escritura)

Valores legales

512

1024

2048

Predeterminado

1024

Descripción

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

---

cfgRacVirtual

Este grupo contiene parámetros para configurar la función de medios virtuales del iDRAC6. Se permite una instancia del grupo. Los apartados siguientes describen los objetos en este grupo.

cfgVirMediaAttached (lectura / escritura)

Valores legales

0 = Desconectar

1 = Conectar

2 = Conectar automáticamente

Predeterminado

0

Descripción

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

iDRAC6 o la CLI. Si asigna el valor de **0** a este objeto, hará que los dispositivos se desconecten del bus USB.

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

cfgVirMediaBootOnce (lectura / escritura)

Valores legales

1 (activado)

0 (desactivado)

Predeterminado

0

Descripción

Activa o desactiva la función de iniciar una vez a partir de los medios virtuales del iDRAC6. Si esta propiedad está activada al momento de reiniciar el servidor host, la función intentará iniciar a partir de los dispositivos de medios virtuales; si hay medios adecuados instalados en el dispositivo.

cfgVirMediaKeyEnable (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la función de memoria de medios virtuales del iDRAC

cfgFloppyEmulation (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgActiveDirectory

Este grupo contiene parámetros para configurar la característica Active Directory del iDRAC6.

cfgADRacDomain (lectura / escritura)

Valores legales

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

Predeterminado

(vacío)

Descripción

El dominio de Active Directory donde reside el DRAC

cfgADRacName (lectura / escritura)

Valores legales

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

Predeterminado

(vacío)

Descripción

El nombre del iDRAC6 como está registrado en el bosque de Active Directory

cfgADEnable (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la autentificación de usuario de Active Directory en iDRAC6. Si esta propiedad está desactivada, se utilizará la autentificación local de iDRAC6 para los inicios de sesión de usuario.

cfgADAuthTimeout (lectura / escritura)

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

Valores legales

De 15 a 300

Predeterminado

120

Descripción

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

cfgADDomainController1 (lectura/escritura)

Valores legales

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

Predeterminado

Ningún valor predeterminado

Descripción

El iDRAC6 utiliza el valor que especifique para buscar nombres de usuario en el servidor LDAP.

cfgADDomainController2 (lectura/escritura)

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

Predeterminado

Ningún valor predeterminado

Descripción

El iDRAC6 utiliza el valor que especifique para buscar nombres de usuario en el servidor LDAP.

cfgADDomainController3 (lectura/escritura)

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

Predeterminado

Ningún valor predeterminado

Descripción

El iDRAC6 utiliza el valor que especifique para buscar nombres de usuario en el servidor LDAP.

cfgADGlobalCatalog1 (lectura/escritura)

Valores legales

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

Predeterminado

Ningún valor predeterminado

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor de catálogo global.

cfgADGlobalCatalog2 (lectura/escritura)

Valores legales

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

Predeterminado

Ningún valor predeterminado

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor de catálogo global.

cfgADGlobalCatalog3 (lectura/escritura)

Valores legales

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

Predeterminado

Ningún valor predeterminado

Descripción

El iDRAC6 usa el valor especificado para buscar nombres de usuario en el servidor de catálogo global.

cfgADType (lectura/escritura)

Valores legales

1 = activa Active Directory con el esquema ampliado

2 = activa Active Directory con el esquema estándar

Predeterminado

1

Descripción

Determina el tipo de esquema que se utiliza con Active Directory

cfgADCertValidationEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Activa o desactiva la validación de certificados de Active Directory

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex (sólo lectura)

Valores legales

De 1 a 5

Descripción

Índice del grupo de funciones como está registrado en Active Directory

cfgSSADRoleGroupName (lectura/escritura)

Valores legales

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

Predeterminado

(vacío)

Descripción

Nombre del grupo de funciones como está registrado en el bosque de Active Directory

cfgSSADRoleGroupDomain (lectura/escritura)

Valores legales

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

Predeterminado

(vacío)

Descripción

El dominio de Active Directory donde reside el grupo de funciones

cfgSSADRoleGroupPrivilege (lectura/escritura)

Valores legales

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

Predeterminado

(vacío)

Descripción

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

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

Privilegio del grupo de funciones	Máscara de bits
Iniciar sesión en el iDRAC6	0x00000001
Configurar el iDRAC6	0x00000002
Configurar usuarios	0x00000004
Borrar registros	0x00000008
Ejecutar comandos de control del servidor	0x00000010
Acceder a redirección de consola	0x00000020
Acceder a los medios virtuales	0x00000040
Probar alertas	0x00000080
Ejecutar comandos de depuración	0x00000100

---

cfgIpmiSol

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

cfgIpmiSolEnable (lectura/escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva SOL

cfgIpmiSolBaudRate (lectura/escritura)

Valores legales

9600, 19200, 57600, 115200

Predeterminado

115200

Descripción

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

cfgIpmiSolMinPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiSolAccumulateInterval (lectura/escritura)

Valores legales

De 1 a 255

Predeterminado

10

Descripción

Especifica la cantidad estándar de tiempo que el iDRAC6 espera antes de transmitir un paquete parcial de datos de caracteres de comunicación en serie en la LAN. Este valor consta de incrementos de 5 ms basados en unos.

cfgIpmiSolSendThreshold (lectura/escritura)

Valores legales

De 1 a 255

Predeterminado

255

Descripción

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

---

cfgIpmiLan

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

cfgIpmiLanEnable (lectura/escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

0

Descripción

Activa o desactiva la interfaz de IPMI en la LAN

cfgIpmiLanPrivLimit (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

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

cfgIpmiLanAlertEnable (lectura/escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

0

Descripción

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

cfgIpmiEncryptionKey (lectura/escritura)

Valores legales

Una cadena de dígitos hexadecimales de 0 a 40 caracteres sin espacios

Predeterminado

0000000000000000000000000000000000000000

Descripción

La clave de cifrado de IPMI

cfgIpmiPetCommunityName (lectura/escritura)

Valores legales

Una cadena de hasta 18 caracteres

Predeterminado

público

Descripción

El nombre de comunidad SNMP para las capturas

---

cfgIpmiPef

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

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

cfgIpmiPefName (sólo lectura)

Valores legales

Una cadena de hasta 255 caracteres

Predeterminado

El nombre del filtro de índice

Descripción

Especifica el nombre del filtro de sucesos de plataforma

cfgIpmiPefIndex (sólo lectura)

Valores legales

De 1 a 17

Predeterminado

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

Descripción

Especifica el índice de un filtro de sucesos de plataforma específico

cfgIpmiPefAction (lectura/escritura)

Valores legales

0 (ninguno)

1 (apagar)

2 (restablecer)

3 (realizar ciclo de encendido)

Predeterminado

0

Descripción

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

cfgIpmiPefEnable (lectura/escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva un filtro de sucesos de plataforma específico.

---

cfgIpmiPet

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

cfgIpmiPetIndex (lectura/escritura)

Valores legales

De 1 a 4

Predeterminado

El valor de índice correspondiente

Descripción

Identificador único para el índice que corresponde a la captura

cfgIpmiPetAlertDestIpAddr (lectura/escritura)

Valores legales

Cadena que representa una dirección IP válida. Por ejemplo, 192.168.0.67.

Predeterminado

0.0.0.0

Descripción

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

cfgIpmiPetAlertEnable (lectura/escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva una captura específica

Regresar a la página de contenido

Regresar a la página de contenido

Base de datos de propiedades SM-CLP del iDRAC6

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

/system1/sp1/account<1-16>

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

userid (sólo lectura)

Valores legales

1-16

Predeterminado

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

Descripción

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

username (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 16

Predeterminado

""

Descripción

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

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

oemdell_ipmilanprivileges (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

15 (Sin acceso)

Predeterminado

4 (Usuario 2)

15 (Todos los demás)

Descripción

El privilegio máximo en el canal de LAN de IPMI.

password (sólo escritura)

Valores legales

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

Predeterminado

""

Descripción

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

enabledstate (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Ayuda a activar o desactivar a un usuario individual.

soleenables (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

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

oemdell_extendedprivileges (lectura/escritura)

Valores legales

De 0x00000000 a 0x000001ff

Predeterminado

0x00000000

Descripción

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

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

Privilegio del usuario	Máscara de bits de privilegios
Iniciar sesión en el iDRAC6	0x0000001
Configurar el iDRAC6	0x0000002
Configurar usuarios	0x0000004
Borrar registros	0x0000008
Ejecutar comandos de control del servidor	0x0000010
Acceder a redirección de consola	0x0000020
Acceder a los medios virtuales	0x0000040
Probar alertas	0x0000080
Ejecutar comandos de depuración	0x0000100

Ejemplos

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

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

Privilegios del usuario	Máscara de bits de privilegios
El usuario no tiene permiso para acceder al iDRAC6.	0x00000000
El usuario sólo puede iniciar sesión en el iDRAC6 y ver la información de configuración del servidor y del iDRAC6.	0x00000001
El usuario puede iniciar sesión en el iDRAC6 y cambiar la configuración.	0x00000001 + 0x00000002 = 0x00000003
El usuario puede iniciar sesión en el RAC, acceder a los medios virtuales y acceder a la redirección de consola.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

/system1/sp1/enetport1/*

Este grupo contiene parámetros para configurar la NIC del iDRAC6. Se permite una instancia del grupo. Todos los objetos en este grupo requerirán que se restablezca la NIC del iDRAC6, lo que puede ocasionar una breve pérdida de la conectividad. Los objetos que cambien la configuración de la dirección IP de la NIC del iDRAC6 cerrarán todas las sesiones de usuario activas y requerirán que los usuarios se vuelvan a conectar con la configuración actualizada de la dirección IP.

macaddress (sólo lectura)

Valores legales

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

Predeterminado

La dirección MAC actual de la NIC del iDRAC6. Por ejemplo, 00:12:67:52:51:A3.

Descripción

Contiene la dirección MAC de la NIC del iDRAC6.

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdell_nicenable (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Activa o desactiva la NIC del iDRAC6. Si la NIC está desactivada, las interfaces de red remotas al iDRAC6 se tornan inaccesibles, lo cual provoca que el iDRAC6 esté disponible solamente mediante la interfaz de RACADM local.

ipaddress (lectura/escritura)

Valores legales

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

Predeterminado

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

Descripción

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

subnetmask (lectura/escritura)

Valores legales

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

Predeterminado

255.255.255.0

Descripción

La máscara de subred que se utiliza para la asignación estática de la dirección IP del iDRAC6. Esta propiedad es válida solamente si oemdell_usedhcp está configurado en 0 (desactivado).

oemdell_usedhcp (lectura / escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Especifica si se utiliza DHCP para asignar la dirección IP del iDRAC6. Si esta propiedad se configura en 1 (Activado), entonces la dirección IP del iDRAC6, la máscara de subred y la puerta de enlace se asignan desde el servidor DHCP de la red. Si esta propiedad se configura en 0 (desactivado), la dirección IP estática, la máscara de subred y la puerta de enlace obtienen valores insertados manualmente por el usuario.

asignado (lectura / escritura)

Valores legales

0 (asignación pendiente)

1 (asignado)

Predeterminado

1

Descripción

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

/system1/sp1/enetport1/lanendpt1/ipendpt1

oemdell_domainnamefromdhcp (lectura / escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Especifica que el nombre del dominio DNS del iDRAC6 se debe asignar desde el servidor DHCP de la red.

oemdell_dnsdomainname (lectura/escritura)

Valores legales

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

Predeterminado

""

Descripción

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

oemdell_dnsregisterrac (lectura/escritura)

Valores legales

0 (no registrado)

1 (registrado)

Predeterminado

0

Descripción

Registra el nombre del iDRAC6 en el servidor DNS.

oemdell_dnsracname (lectura/escritura)

Valores legales

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

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

Predeterminado

rac-etiqueta_de_servicio

Descripción

Muestra el nombre de RAC, que es la etiqueta de servicio RAC predeterminada. Este parámetro es válido solamente si oemdell_dnsregisterrac está configurado en 1 (Registrado).

oemdell_serversfromdhcp (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

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

/system1/sp1/enetport1/lanendpt1/ipendpt1

dnsserveraddress (lectura/escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

/system1/sp1/enetport1/lanendpt1/ipendpt1

dnsserveraddress (lectura/escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

/system1/sp1/enetport1/lanendpt1/ipendpt1

defaultgatewayaddress (lectura/escritura)

Valores legales

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

Predeterminado

192.168.0.1

Descripción

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

/system1/sp1/group<1-5>

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

oemdell_groupname (lectura/escritura)

Valores legales

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

Predeterminado

""

Descripción

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

oemdell_groupdomain (lectura/escritura)

Valores legales

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

Predeterminado

""

Descripción

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

oemdell_groupprivilege (lectura/escritura)

Valores legales

De 0x00000000 a 0x000001ff

Predeterminado

""

Descripción

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

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

Grupo de funciones	Máscara de bits de privilegios
Iniciar sesión en el iDRAC6	0x00000001
Configurar el iDRAC6	0x00000002
Configurar usuarios	0x00000004
Borrar registros	0x00000008
Ejecutar comandos de control del servidor	0x00000010
Acceder a redirección de consola	0x00000020
Acceder a los medios virtuales	0x00000040
Probar alertas	0x00000080
Ejecutar comandos de depuración	0x00000100

/system1/sp1/oemdell_adservice1

Este grupo contiene parámetros para configurar la característica Active Directory del iDRAC6.

enabledstate (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Activa o desactiva la autentificación de usuario de Active Directory en iDRAC6. Si esta propiedad está desactivada, se usará la autentificación local del iDRAC6 para los inicios de sesión de usuarios.

oemdell_adracname (lectura/escritura)

Valores legales

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

Predeterminado

""

Descripción

Nombre del iDRAC6, según está registrado en el bosque de Active Directory.

oemdell_adracdomain (lectura/escritura)

Valores legales

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

Predeterminado

""

Descripción

El dominio de Active Directory en donde reside el iDRAC6.

oemdell_adrootdomain (lectura/escritura)

Valores legales

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

Predeterminado

""

Descripción

Dominio raíz del bosque de dominios.

oemdell_timeout (lectura/escritura)

Valores legales

De 15 a 300

Predeterminado

120

Descripción

Especifica 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.

oemdell_schematype (lectura/escritura)

Valores legales

1 (esquema extendido)

2 (esquema estándar)

Predeterminado

1

Descripción

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

oemdell_adspecifyserverenable (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Permite al usuario especificar un servidor LDAP o Catálogo global.

oemdell_addomaincontroller (lectura/escritura)

Valores legales

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

Predeterminado

""

Descripción

Valor especificado por el usuario que el iDRAC6 usa para buscar nombres de usuarios en el servidor LDAP.

oemdell_adglobalcatalog (lectura/escritura)

Valores legales

Una dirección IP válida para un FQDN.

Predeterminado

Ningún valor predeterminado

Descripción

Valor especificado por el usuario que el iDRAC6 usa para buscar nombres de usuarios en el servidor de Catálogo global.

/system1/sp1/oemdell_racsecurity1

Este grupo se usa para configurar los valores relacionados con la función de solicitud de firma de certificado (CSR) SSL del iDRAC6. Las propiedades en este grupo se deben configurar antes de generar una CSR a partir del iDRAC6.

commonname (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

organizationname (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

oemdell_organizationunit (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

oemdell_localityname (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica la localidad de la CSR.

oemdell_statename (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el nombre común de la CSR.

oemdell_countrycode (lectura/escritura)

Valores legales

Una cadena de hasta 2 caracteres ASCII.

Predeterminado

""

Descripción

Especifica el código de país de la CSR.

oemdell_emailaddress (lectura/escritura)

Valores legales

Una cadena de hasta 254 caracteres ASCII.

Predeterminado

""

Descripción

Especifica la dirección de correo electrónico de CSR.

oemdell_keysize (lectura/escritura)

Valores legales

1024

2048

4 096

Predeterminado

1024

Descripción

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

/system1/sp1/oemdell_ssl1

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

generate (lectura/escritura)

Valores legales

0 (no generar)

1 (generar)

Predeterminado

0

Descripción

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

oemdell_status (sólo lectura)

Valores legales

No se encuentra CSR

CSR generada

Predeterminado

No se encuentra CSR

Descripción

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

oemdell_certtype (lectura/escritura)

Valores legales

SSL

AD

CSR

Predeterminado

SSL

Descripción

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

/system1/sp1/oemdell_vmservice1

Este grupo contiene parámetros para configurar la función de medios virtuales del iDRAC6.

enabledstate (lectura/escritura)

Valores legales

VMEDIA_DETACH

VMEDIA_ATTACH

VMEDIA_AUTO_ATTACH

Predeterminado

VMEDIA_ATTACH

Descripción

Se usa para conectar dispositivos virtuales al sistema mediante el bus USB, permitiendo al servidor reconocer dispositivos de almacenamiento masivo USB conectados al sistema. Esto equivale a conectar una unidad de disco flexible o una unidad de CD-ROM USB local a un puerto USB del sistema. Cuando los dispositivos están conectados, es posible conectar los dispositivos virtuales de manera remota mediante la interfaz web del iDRAC6 o la CLI. Si asigna el valor de 0 a esta propiedad, hará que los dispositivos se desconecten del bus USB.

oemdell_singleboot (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

Activa o desactiva la función de iniciar una vez a partir de los medios virtuales del iDRAC6. Si esta propiedad está desactivada cuando se reinicia el servidor host, el servidor intentará reiniciarse de todos los dispositivos multimedia virtuales.

oemdell_floppyemulation (lectura/escritura)

Valores legales

0 (desactivado)

1 (activado)

Predeterminado

0

Descripción

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

/system1/sp1/oemdell_vmservice1/tcpendpt1

portnumber (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

3668

Descripción

Especifica el número de puerto que se usa para las conexiones cifradas de medios virtuales con el iDRAC6.

oemdell_sslenabled (sólo lectura)

Valor legal

FALSE

Predeterminado

FALSE

Descripción

Indica que el puerto tiene SSL desactivado.

portnumber (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

3670

Descripción

Especifica el número de puerto que se usa para las conexiones cifradas de medios virtuales con el iDRAC6.

oemdell_sslenabled (sólo lectura)

Valor legal

TRUE

Predeterminado

TRUE

Descripción

Indica que el puerto tiene SSL desactivado.

Regresar a la página de contenido

Regresar a la página de contenido

Equivalencias de RACADM y SM-CLP

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

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

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

Grupos y objetos de RACADM	SM-CLP	Descripción
idRacInfo		
idRacName		Cadena de hasta 15 caracteres ASCII. Valor predeterminado: **iDRAC**.
idRacProductInfo		Cadena de hasta 63 caracteres ASCII. Valor predeterminado: **Integrated Dell Remote Access Controller**.
idRacDescriptionInfo		Cadena de hasta 255 caracteres ASCII Valor predeterminado: **Este componente de sistema proporciona un conjunto completo de funciones de administración remota para los servidores Dell PowerEdge**
idRacVersionInfo		Cadena de hasta 63 caracteres ASCII. Valor predeterminado: **1**
idRacBuildInfo		Cadena de hasta 16 caracteres ASCII.
idRacType		Valor predeterminado: **8**
cfgActiveDirectory	**/system1/sp1/ oemdell_adservice1**	
cfgADEnable	enablestate	0 para desactivar, 1 para activar. Valor predeterminado: **0**
cfgADRacName	oemdell_adracname	Una cadena de hasta 254 caracteres.
cfgADRacDomain	oemdell_adracdomain	Una cadena de hasta 254 caracteres.
cfgADAuthTimeout	oemdell_timeout	De 15 a 300 segundos. Valor predeterminado: **120**
cfgADType	oemdell_schematype	1 para esquema estándar, 2 para esquema extendido. Valor predeterminado: **1**
cfgADDomainController	oemdell_addomaincontroller	El nombre DNS o la dirección IP del controlador de dominio que se usa en la búsqueda de LDAP
cfgADGlobalCatalog	oemdell_adglobalcatalog	El nombre DNS o la dirección IP del servidor de catálogo global que se usa en la búsqueda de LDAP
cfgStandardSchema		
cfgSSADRoleGroupIndex	**/system1/sp1/group1** *a* **/system1/sp1/group5**	RACADM: identificación de índice de grupo (1-5) SM-CLP: se selecciona con la ruta de acceso de la dirección
cfgSSADRoleGroupName	oemdell_groupname	Una cadena de hasta 254 caracteres
cfgSSADRoleGroupDomain	oemdell_groupdomain	Una cadena de hasta 254 caracteres
cfgSSADRoleGroupPrivilege	oemdell_grouppprivilege	Máscara de bits con valores entre 0x00000000 y 0x000001ff
cfgLanNetworking	**/system1/sp1/enetport1**	
cfgNicMacAddress	macaddress	La dirección MAC de la interfaz. No se puede editar
	/system1/sp1/enetport1 /lanendpt1/ipendpt1	
cfgNicEnable	oemdell_nicenable	**0** para desactivar la NIC, 1 para activar la NIC Valor predeterminado: **0**
cfgNicUseDHCP	oemdell_usedhcp	**0** para configurar direcciones de red estáticas, 1 para usar DHCP Valor predeterminado: **0**
cfgNicIpAddress	ipaddress	La dirección IP predeterminada del iDRAC6 es: **192.168.0.120** más el número de ranura del servidor.
cfgNicNetmask	subnetmask	La máscara de subred para la red predeterminada del iDRAC6 es: **255.255.255.0**
	comprometidos	Cuando los valores del grupo cambian, **committed** tiene el valor 0 para indicar que los nuevos valores no han sido guardados. Establezca el valor en **1** para guardar la nueva configuración. Valor predeterminado: **1**
	/system1/sp1/enetport1/lanendpt1/	

	ipendpt1	
cfgDNSDomainName	oemdell_dnsdomainname	Cadena de hasta 250 caracteres ASCII. Al menos un carácter debe ser alfabético.
cfgDNSDomainNameFromDHCP	oemdell_domainnamefromdhcp	Establezca el valor 1 para obtener el nombre de dominio de DHCP. Valor predeterminado: **0**
cfgDNSRacName	oemdell_dnsracname	Cadena de hasta 63 caracteres ASCII. Al menos un carácter debe ser alfabético. Valor predeterminado: **iDRAC-** *más la etiqueta de servicio de Dell*.
cfgDNSRegisterRac	oemdell_dnsregisterrac	Establezca el valor en 1 para registrar el nombre del iDRAC6 en el DNS. Valor predeterminado: **0**
cfgDNSServersFromDHCP	oemdell_dnsserversfromdhcp	Establezca el valor en 1 para obtener del DHCP Default las direcciones de servidor DN**S** Valor predeterminado: **0**
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgDNSServer1	dnsserveraddresses1	Una cadena que representa la dirección IP de un servidor DNS
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgDNSServer2	dnsserveraddresses2	Una cadena que representa la dirección IP de un servidor DNS
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgNicGateway	defaultgatewayaddress	Una cadena que representa la dirección IP del gateway Valor predeterminado: **192.168.0.1**
cfgRacVirtual	**/system1/sp1/oemdell_vmservice1**	
cfgFloppyEmulation	oemdell_floppyemulation	Establezca el valor en 1 para activar la emulación de disco flexible. Valor predeterminado: **0**
cfgVirMediaAttached	enabledstate	Establezca el valor en 1 (RACADM)/VMEDIA_ATTACH (SM-CLP) para contectar los medios. Valor predeterminado: 1 (RACADM)/VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdell_singleboot	Establezca el valor en 1 para ejecutar el siguiente inicio desde los medios seleccionados Valor predeterminado: **0**
	/system1/sp1/oemdell_vmservice1/tcpendpt1	
	oemdell_sslenabled	Establezca el valor en 1 si SSL está activado para el primer dispositivo de medios virtuales y en 0 si no es así. No se puede editar
cfgVirAtapiSvrPort	portnumber	Puerto para uso del primer dispositivo de medios virtuales. Valor predeterminado: **3668**
	/system1/sp1/oemdell_vmservice1/tcpendpt2	
	oemdell_sslenabled	Establezca el valor en 1 si SSL está activado para el segundo dispositivo de medios virtuales y en 0 si no es así. No se puede editar
cfgVirAtapiSvrPortSsl	portnumber	Puerto para uso del primer dispositivo de medios virtuales. Valor predeterminado: **3670**
cfgUserAdmin	**/system1/sp1/account1** ***a*** **/system1/sp1/account16**	
cfgUserAdminEnable	enabledstate	Establezca el valor en 1 para activar el usuario. Valor predeterminado: **0**
cfgUserAdminIndex	userid	Índice de usuario, de 1 a 16
cfgUserAdminIpmiLanPrivilege	oemdell_ipmilanprivileges	2 (usuario), 3 (operador), 4 (administrador) o 15 (sin acceso) Valor predeterminado: **4**
cfgUserAdminPassword	contraseña	Una cadena de hasta 20 caracteres ASCII
cfgUserAdminPrivilege	oemdell_extendedprivileges	El valor de la máscara de bits entre 0x00000000 y 0x000001ff Valor predeterminado: **0x00000000**
cfgUserAdminSolEnable	solenabled	Establezca el valor en 1 para permitir que el usuario use comunicación en serie en la LAN. Valor predeterminado: **0**
cfgUserAdminUserName	nombre de usuario	Cadena de hasta 16 caracteres
cfgEmailAlert		
cfgEmailAlertAddress		Dirección de destino de correo electrónico, de hasta 64 caracteres

cfgEmailAlertCustomMsg		Mensaje para enviar en correo electrónico, hasta 32 caracteres
cfgEmailAlertEnable		Establezca el valor en 1 para activar la alerta por correo electrónico Valor predeterminado: **0**
cfgEmailAlertIndex		Índice de una instancia de alerta por correo electrónico. Número de 1 a 4
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		Cantidad de sesiones simultáneas permitidas de redirección de consola (1 ó 2). Valor predeterminado: **2**
cfgSsnMgtSshIdleTimeout		Número de segundos de inactividad antes que la sesión SSH agote el tiempo de espera. 0 para desactivar el tiempo de espera o para establecerlo entre 60 y 1920 segundos. Valor predeterminado: **300**
cfgSsnMgtTelnetIdleTimeout		Número de segundos de inactividad antes de que la sesión de Telnet agote el tiempo de espera. 0 para desactivar el tiempo de espera o para establecerlo entre 60 y 1920 segundos. Valor predeterminado: **300**
cfgSsnMgtWebserverTimeout		Número de segundos de inactividad antes de que la sesión de interfaz web agote el tiempo de espera. De 60 a 1920 segundos. Valor predeterminado: **300**
cfgRacTuning		
cfgRacTuneConRedirEnable		Establezca el valor en 1 para activar la redirección de consola o en 0 para desactivarla Valor predeterminado: **1**
cfgRacTuneConRedirEncrypt Enable		Establezca el valor en 1 para activar el cifrado del tráfico de red de la redirección de consola o en 0 para desactivarlo. Valor predeterminado: **1**
cfgRacTuneConRedirPort		Puerto que se va a usar para la redirección de la consola. Valor predeterminado: **5900**
cfgRacTuneConRedirVideoPort		Puerto que se va a usar para la redirección de vídeo de la consola. Valor predeterminado: **5901**
cfgRacTuneHttpPort		Puerto que se va a usar para la interfaz web de HTTP. Valor predeterminado: **80**
cfgRacTuneHttpsPort		Puerto que se va a usar para la interfaz web de HTTPS. Valor predeterminado: **443**
cfgRacTuneIpBlkEnable		Establezca el valor en 1 para bloquear la IP Valor predeterminado: **0**
cfgRacTuneIPBlkFailCount		El número de intentos fallidos de inicio de sesión permitidos antes de bloquear la IP (de 2 a 16). Valor predeterminado: **5**
cfgRacTuneIpBlkFailWindow		Periodo en segundos durante el cual se cuentan los intentos fallidos de inicio de sesión (de 10 a 65535) Valor predeterminado: **60**
cfgRacTuneIpBlkPenaltyTime		El periodo en segundos que una IP permanecerá bloqueada (de 10 a 65535) Valor predeterminado: **300**
cfgRacTuneIpRangeAddr		La dirección base para el filtro de rango de IP Valor predeterminado: **192.168.0.1**
cfgRacTuneIpRangeEnable		Establezca el valor en 1 para activar la filtración de rango de IP Valor predeterminado: 0
cfgRacTuneIpRangeMask		Máscara de bits aplicada a la dirección base para seleccionar direcciones IP válidas. Valor predeterminado: **255.255.255.0**
cfgRacTuneLocalServerVideo		Establezca el valor en 1 para activar la consola iKVM local Valor predeterminado: **1**
cfgRacTuneSshPort		Puerto para uso del servicio SSH Valor predeterminado: **22**
cfgRacTuneTelnetPort		Puerto para uso del servicio Telnet Valor predeterminado: **23**
cfgRacTuneWebserverEnable		Establezca el valor en 1 para activar la interfaz web del iDRAC6. Valor predeterminado: **1**
ifcRacManagedNodeOS		
ifcRacMnOsHostname		El nombre de host del servidor administrado. Una cadena de hasta 255 caracteres
ifcRacMnOsOsName		Nombre del sistema operativo del servidor administrado. Una cadena de hasta 255 caracteres
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Nombre común de Active Directory. Una cadena de hasta 254 caracteres
cfgRacSecCsrCountryCode	oemdell_countrycode	Código de país de Active Directory. Dos caracteres
cfgRacSecCsrEmailAddr	oemdell_emailaddress	Dirección de correo electrónico que se usa para la solicitud de firma de certificado. Una cadena de hasta 254 caracteres

cfgRacSecCsrKeySize	oemdell_keysize	Longitud de la clave de cifrado (512, 1024 ó 2048). Valor predeterminado: **1024**
cfgRacSecCsrLocalityName	oemdell_localityname	Nombre de la localidad de Active Directory. Una cadena de hasta 254 caracteres
cfgRacSecCsrOrganizationName	organizationname	Nombre de organización de Active Directory. Una cadena de hasta 254 caracteres
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Nombre de la unidad de organización de Active Directory. Una cadena de hasta 254 caracteres
cfgRacSecCsrStateName	oemdell_statename	Nombre del estado de Active Directory. Una cadena de hasta 254 caracteres
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		Cantidad máxima de milisegundos que se debe esperar antes del envío de un paquete parcial de comunicación en serie en la LAN (de 1 a 255) Valor predeterminado: **10**
cfgIpmiSolBaudRate		Velocidad en baudios para uso en la comunicación en serie en la LAN (19200, 57600, 115200). Valor predeterminado: **115200**
cfgIpmiSolEnable		Establezca el valor en 1 para activar la función se comunicación en serie en la LAN. Valor predeterminado: **0**
cfgIpmiSolSendThreshold		Cantidad máxima de caracteres que se deben recopilar antes del envío de datos de SOL (de 1 a 255) Valor predeterminado: **255**
cfgIpmiSolMinPrivilege		Privilegio mínimo requerido para usar la comunicación en serie en la LAN. 2 (usuario), 3 (operador) o 4 (administrador) Valor predeterminado: **4**
cfgIpmiLan		
cfgIpmiEncryptionKey		Una cadena de 0 a 40 dígitos hexadecimales. Valor predeterminado: **0000000000000000000000000000000000000000**
cfgIpmiLanAlertEnable		Establezca el valor en 1 para activar las alertas de LAN IPMI Valor predeterminado: **0**
cfgIpmiLanEnable		Establezca el valor en 1 para activar IPMI en la interfaz de LAN Valor predeterminado: **0**
cfgIpmiPetCommunityName		Una cadena de 18 caracteres. Valor predeterminado: **public**
cfgIpmiPef		
cfgIpmiPefAction		La acción a realizar al detectar el suceso. 0 (ninguna), 1 (apagar), 2 (restablecer), 3 (ciclo de encendido). Valor predeterminado: **0**
cfgIpmiPefEnable		Establezca el valor en 1 para activar el filtro de sucesos de plataforma. Valor predeterminado: **0**
cfgIpmiPefIndex		El número índice del filtro de sucesos de plataforma. (1 - 17)
cfgIpmiPefName		El nombre del suceso de plataforma, una cadena de hasta 254 caracteres. No se puede editar
cfgIpmiPet		
cfgIpmiPetAlertDestIpAddr		La dirección IP del receptor de captura de sucesos de plataforma. Valor predeterminado: **0.0.0.0**
cfgIpmiPetAlertEnable		Establezca el valor en 1 para activar la captura de sucesos de plataforma. Valor predeterminado: **1**
cfgIpmiPetIndex		Número índice (de 1 a 4) de la captura de sucesos de plataforma

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

Subcomando de RACADM	SM-CLP	Descripción
sslcsrgen -g	set /system1/sp1/oemdell_ssl1 oemdell_certtype=CSR set /system1/sp1/oemdell_ssl1 generate=1 dump -destination <URI_de_TFTP_de_solicitud_de_firma_de_certificado_del_iDRAC> /system1/sp1/oemdell_ssl1	Genera y descarga una solicitud de firma de certificado (CSR) SSL
sslcsrgen -s	show /system1/sp1/oemdell_ssl1 oemdell_status	Indica el estado del proceso de generación de la CSR
sslcertupload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <URI_de_TFTP_de_certificado_de_servidor_del_iDRAC> /system1/sp1/oemdell_ssl1	Carga el certificado del servidor del iDRAC6 en el iDRAC6
sslcertupload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <URI_de_TFTP_de_certificado_de_ActiveDirectory> /system1/sp1/oemdell_ssl1	Carga el certificado Active Directory en iDRAC6

sslcertdownload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <URI_de_TFTP_de_certificado_de_servidor_del_iDRAC> /system1/sp1/oemdell_ssl1	Descarga el certificado del servidor del iDRAC6 desde el iDRAC6
sslcertdownload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <URI_de_TFTP_de_certificado_de_ActiveDirectory> /system1/sp1/oemdell_ssl1	Descarga el certificado de Active Directory desde el iDRAC6

Regresar a la página de contenido

Regresar a la página de contenido

Descripción general del iDRAC6 Enterprise

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Integrated Dell™ Remote Access Controller (iDRAC6) es una solución de hardware y software de administración de sistemas que brinda capacidades de administración remota, recuperación de sistemas bloqueados y funciones de control de alimentación para los sistemas Dell PowerEdge™.

iDRAC6 utiliza un microprocesador integrado de sistema en chip para el sistema de control y supervisión remoto, y coexiste en la placa base con el servidor PowerEdge administrado. El sistema operativo del servidor se encarga de las aplicaciones de ejecución; el iDRAC6 se encarga de la supervisión y administración del entorno y el estado del servidor fuera del sistema operativo.

Se puede configurar el iDRAC6 para que éste le envíe alertas por correo electrónico o alertas de captura de Protocolo simple de administración de red (SNMP) ante advertencias o errores. Para ayudar a diagnosticar la causa probable de un bloqueo de sistema, iDRAC6 puede registrar datos de suceso y capturar una imagen de la pantalla cuando detecta que el sistema se ha bloqueado.

Los servidores administrados están instalados en un gabinete (chasis) de sistema Dell M1000e con suministros de energía modulares, ventiladores y un controlador de administración de chasis (CMC). El CMC supervisa y administra todos los componentes instalados en el chasis. Se puede agregar un CMC redundante para estar protegido contra fallas en caso de que el CMC principal falle. El chasis ofrece acceso a los dispositivos iDRAC6 por medio de la pantalla LCD, las conexiones de consola locales y la interfaz web.

Todas las conexiones de red al iDRAC6 son a través de la interfaz de red del CMC (el puerto de conexión RJ45 del CMC etiquetado "Gb"). El CMC enruta el tráfico hacia los dispositivos iDRAC6 en los servidores por medio de una red privada interna. Esta red de administración privada está fuera de la ruta de datos del servidor y fuera del control del sistema operativo, es decir *fuera de banda*. Se puede acceder a las interfaces de red *dentro de banda* de los servidores administrados mediante los módulos de E/S (IOM) instalados en el chasis.

De manera predeterminada, la interfaz de red del iDRAC6 está desactivada. Se debe configurar antes de que se pueda acceder al iDRAC6. Una vez que el iDRAC6 esté activado y configurado en la red, se podrá tener acceso a la dirección IP asignada de éste por medio de la interfaz web del iDRAC6, Telnet o SSH y de los protocolos de administración de red admitidos, como la Interfaz de administración de plataforma inteligente (IPMI).

Funciones de administración del iDRAC6

iDRAC6 proporciona las siguientes funciones de administración:

- Registro de Sistema dinámico de nombres de dominio (DDNS)
- Administración y supervisión de sistemas remotos por medio de una interfaz web, la interfaz de línea de comandos RACADM local a través de la redirección de consola y la línea de comandos SM-CLP mediante una conexión Telnet/SSH
- Compatibilidad con la autentificación de Microsoft Active Directory®: centraliza las identificaciones y contraseñas de usuario de iDRAC6 en Active Directory por medio del esquema estándar o de un esquema ampliado
- Redirección de consola: proporciona funciones remotas de teclado, vídeo y ratón
- Medios virtuales: activa un servidor administrado para tener acceso a una unidad local de medios en la estación de administración o a imágenes ISO de CD/DVD en un recurso compartido de red
- Supervisión: brinda acceso a la información del sistema y al estado de los componentes
- Acceso a los registros del sistema: brinda acceso al registro de sucesos del sistema, el registro del iDRAC6 y la última pantalla de bloqueo del sistema bloqueado o que no responde que es independiente del estado del sistema operativo
- Integración del software de Dell OpenManage™: permite iniciar la interfaz web del iDRAC6 desde Dell OpenManage Server Administrator o IT Assistant
- Captura de inicio: brinda hasta tres pantallas de captura de inicio para depuración posterior
- Alerta de iDRAC6: alerta sobre problemas potenciales del nodo administrado por medio de un mensaje por correo electrónico o una captura SNMP
- Administración remota de la alimentación: brinda funciones de administración remota de la alimentación, como el apagado y restablecimiento, a partir de una consola de administración
- Inicio de sesión único desde la interfaz web del CMC: una vez que se registra al CMC, puede acceder a cualquier IDRAC6 del chasis sin tener que registrarse nuevamente
- Una a varias actualizaciones de firmware: permite la actualización automatizada de más de un iDRAC6 sin intervención del operador
- Compatibilidad con la Interfaz de administración de plataforma inteligente (IPMI)
- Cifrado de Capa de conexión segura (SSL): ofrece administración remota y segura de sistemas por medio de la interfaz web
- Administración de seguridad de nivel de contraseña: evita el acceso no autorizado a un sistema remoto
- Autoridad en base a funciones: proporciona permisos asignables para distintas tareas de administración de sistemas

---

Características de seguridad del iDRAC6

iDRAC6 proporciona las siguientes funciones de seguridad:

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

  NOTA: Telnet no admite el cifrado SSL.

- Secure Shell (SSH), que usa una capa de transporte cifrado para ofrecer mayor seguridad
- Límites de falla de inicio de sesión por dirección IP, con bloqueo del inicio de sesión de la dirección IP cuando ésta ha superado el límite
- Rango limitado de direcciones IP para clientes que se conectan al iDRAC6

Mejoras del firmware del iDRAC6

Además, se han realizado importantes mejoras al código:

- Importantes mejoras en la función de búsqueda de Active Directory
- Mejor capacidad de respuesta de la pila de red TCP-IP
- Mejor interfaz de estado de condición general entre iDRAC6 y CMC
- Mejoras de seguridad por medio de varias herramientas de análisis de terceros

---

Plataformas admitidas

El iDRAC6 admite los siguientes sistemas PowerEdge en el gabinete del sistema Dell PowerEdge M1000e:

- PowerEdge M610
- PowerEdge M710

Consulte el archivo léame del iDRAC6 ubicado en el sitio web de asistencia de Dell, en **support.dell.com/manuals**, para ver las plataformas admitidas más recientes.

Sistemas operativos admitidos

La tabla 1-1 muestra una lista de los sistemas operativos que admiten el iDRAC6.

Consulte la *Matriz de compatibilidad de software de los sistemas Dell* que se encuentra en el sitio web de asistencia de Dell en **support.dell.com/manuals** para ver la información más reciente.

Tabla 1-1. Sistemas operativos admitidos

Familia de sistemas operativos	Sistema operativo
Microsoft® Windows®	Microsoft Windows Server®2003 R2 ediciones Standard y Enterprise (x86 de 32 bits) con SP2 Microsoft Windows Server 2003 ediciones Standard y Enterprise (x86 de 32 bits) con SP2 Microsoft Windows Server 2003 Standard Edition y Enterprise (x64) Edition con SP2 Microsoft Windows Storage Server 2003 R2, ediciones Express, Workgroup, Standard y Enterprise x64 Microsoft Windows Server 2008 ediciones Web, Standard y Enterprise (x86 de 32 bits) Microsoft Windows Server 2008 ediciones Web, Standard, Enterprise y Datacenter (x64) MS HyperV 2008 **NOTA:** Al instalar Windows Server 2003 con Service Pack 1, tenga en cuenta los cambios de la configuración de seguridad de DCOM. Para obtener más información, consulte el artículo 903220 en el sitio web de asistencia técnica de Microsoft en **support.microsoft.com/kb/903220**.

Red Hat® Enterprise Linux®	Enterprise Linux WS, ES y AS (versión 4) (x86 y x86_64) Enterprise Linux 5 (x86 y x86_64)
SUSE® Linux	Enterprise Server 10 (Gold) (x86_64).
VMware	ESX 3.5 U4

Exploradores web admitidos

La tabla 1-2 presenta una lista de los exploradores web que se admiten como clientes del iDRAC6.

Consulte el archivo Léame y la *Matriz de compatibilidad de software de los sistemas Dell* que se encuentra en el sitio web de asistencia técnica de Dell en **support.dell.com/manuals** para ver la información más reciente.

NOTA: A causa de defectos serios de seguridad, se ha interrumpido la compatibilidad con SSL 2.0. A fin de que su explorador funcione correctamente, deberá activar SSL 3.0.

Tabla 1-2. Exploradores de web compatibles

Sistema operativo	Explorador de web admitido
Windows	Internet Explorer® 6.0 con Service Pack 2 (SP2) para Windows XP y Windows 2003 R2 SP2 únicamente Internet Explorer 7.0 para Windows Vista®, Windows XP, Windows 2003 R2 SP2 y Windows Server 2008 solamente Mozilla Firefox 2.0/3.0 para Windows (consola Java vKVM/vMedia solamente)
Linux	Mozilla Firefox 2.0/3.0 en Red Hat Enterprise Linux 4 y 5 (de 32 bits o 64 bits) y SUSE Linux Enterprise Server 10 (de 32 bits o 64 bits)

Conexiones de acceso remoto admitidas

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

Tabla 1-3. Conexiones de acceso remoto admitidas

Conexión	Características
NIC del iDRAC6	• Ethernet de 10 Mbps/100 Mbps/1 Gbps a través del puerto Gb Ethernet del CMC • Compatibilidad con DHCP • Notificación de sucesos de correo electrónico y capturas SNMP • Compatibilidad para el shell de comandos de SM-CLP (Telnet o SSH) para operaciones como la configuración del iDRAC6, el inicio del sistema, el restablecimiento, el encendido y los comandos de apagado • Compatibilidad para las utilidades de IPMI, como IPMItool e ipmish

Puertos del iDRAC6

La tabla 1-4 muestra una lista de los puertos en los que el iDRAC6 detecta las conexiones. La tabla 1-5 identifica los puertos que el iDRAC6 usa como cliente. Esta información es necesaria cuando se abren servidores de seguridad para permitir el acceso remoto a un iDRAC6.

Tabla 1-4. Puertos en los que el iDRAC6 detecta servidores

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

Tabla 1-5. Puertos de cliente del iDRAC6

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

Otros documentos útiles

Además de esta *Guía del usuario*, los siguientes documentos proporcionan información adicional sobre la configuración y el funcionamiento del iDRAC6 en el sistema:

- La ayuda en línea para el iDRAC6 proporciona información sobre el uso de la interfaz web.
- La *Guía del usuario del firmware del Dell Chassis Management Controller versión 2.0* y la *Guía de referencia del Administrator del firmware del Dell Chassis Management Controller versión 2.0* suministran información acerca del uso del controlador que administra todos los módulos en el chasis que contiene el servidor PowerEdge.
- La *Guía del usuario de Dell OpenManage IT Assistant* contiene información sobre cómo usar IT Assistant.
- La *Guía del usuario de Dell OpenManage Server Administrator* contiene información sobre cómo instalar y usar Server Administrator.
- La *Guía del usuario de Dell Update Packages* contiene información acerca de cómo obtener y usar Dell Update Packages como parte de su estrategia de actualización del sistema.
- La *Guía del usuario de Dell Unified Server Configurator* contiene información sobre cómo instalar y usar Unified Server Configurator.

Los siguientes documentos del sistema también están disponibles para proporcionar más información sobre el sistema en el que iDRAC6 está instalado:

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

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

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

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de iDRAC6 Enterprise

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Esta sección contiene información sobre cómo establecer el acceso al iDRAC6 y configurar el entorno de administración para usarlo.

Antes de comenzar

Reúna los siguientes elementos antes de configurar el iDRAC6:

- *Guía del usuario del firmware Dell del Chassis Management Controller*
- DVD Dell Systems Management Tools and Documentation

El DVD *Dell Systems Management Tools and Documentation* incluye los siguientes componentes:

- Directorio raíz del DVD: contiene Dell Systems Build and Update Utility, que proporciona información sobre la instalación del servidor y del sistema.
- SYSMGMT: contiene productos de software de administración de sistemas, incluso Dell OpenManage Server Administrator
- DOCS: contiene documentación para productos de software de administración de sistemas, periféricos y controladores RAID
- SERVICE: contiene las herramientas que necesita para configurar el sistema, y los últimos diagnósticos y controladores optimizados por Dell para el sistema

Para obtener más información, consulte la *Guía del usuario de Server Administrator*, la *Guía del usuario de IT Assistant* y la *Guía del usuario de Unified Server Configurator*, disponibles en el sitio Web de asistencia de Dell: **support.dell.com\manuals**.

Interfaces para configurar el iDRAC6

Puede configurar el iDRAC6 a través de la utilidad de configuración del iDRAC6, la interfaz Web del iDRAC6, la CLI de RACADM local o la CLI de SM-CLP. La CLI de RACADM local está disponible después haber instalado el sistema operativo y el software Dell OpenManage en el servidor administrado. La tabla 2-1 describe estas interfaces.

Para mayor seguridad, el acceso a la configuración de iDRAC6 a través de la utilidad de configuración del iDRAC6 puede desactivarse con un comando RACADM (consulte "Generalidades del subcomando RACADM") o desde la interfaz gráfica para el usuario (consulte"Activación o desactivación del acceso a la configuración local").

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

Tabla 2-1. Interfaces de configuración

Interfaz	Descripción
Utilidad de configuración del iDRAC6	Se accede a la utilidad de configuración del iDRAC6 al momento del inicio, y es una herramienta útil cuando se instala un nuevo servidor PowerEdge. Úsela para configurar la red y las funciones básicas de seguridad, así como para habilitar otras funciones.
Interfaz Web del iDRAC6	La interfaz Web del iDRAC6 es una aplicación de administración a la que se accede por medio de explorador y que se puede usar para administrar el iDRAC6 de manera interactiva y supervisar al servidor administrado. Es la interfaz principal para las tareas cotidianas, como la supervisión de la condición de sistema, la consulta del registro de sucesos del sistema, la administración de usuarios locales del iDRAC6 y la ejecución de la interfaz Web del CMC y las sesiones de redirección de consola.
Interfaz web del CMC	Además de supervisar y administrar el chasis, la interfaz Web del CMC se puede usar para ver el estado de un servidor administrado, configurar los valores de la red de iDRAC6 e iniciar, detener o restablecer el servidor administrado.
Panel LCD del chasis	El panel LCD en el chasis que contiene el iDRAC6 se puede usar para ver el estado general de los servidores en el chasis. Durante la configuración inicial del CMC, el asistente de configuración permite activar la configuración de DHCP del sistema de red del iDRAC6.
RACADM local	La interfaz de línea de comandos de RACADM local se ejecuta en el servidor administrado. Se accede a ella a través del conmutador iKVM o de una sesión de redirección de consola iniciada desde la interfaz Web de iDRAC6. RACADM se instala en el servidor administrado cuando usted instala Dell OpenManage Server Administrator. Los comandos de RACADM proporcionan acceso a casi todas las funciones de iDRAC6. Usted puede inspeccionar datos de sensor, anotaciones del registro de sucesos de sistema y el estado actual y los valores de configuración que se mantienen en el iDRAC6. También puede cambiar los valores de configuración del iDRAC6, administrar usuarios locales, activar y desactivar funciones y realizar acciones de alimentación como apagar o reiniciar el servidor administrado.
iVMCLI	La interfaz de línea de comandos de medios virtuales del iDRAC6 (iVM-CLI) proporciona al servidor administrado acceso a los medios que se encuentran en la estación de administración. Es útil para desarrollar secuencias de comandos para instalar sistemas operativos en varios servidores administrados.
SM-CLP	SM-CLP es la implementación incorporada en el iDRAC6 del Protocolo de línea de comandos de administración de servidor (SM-CLP) del

	grupo de trabajo de administración de servidor. A la línea de comandos de SM-CLP se accede mediante un inicio de sesión en el iDRAC6 a través de Telnet o SSH. Los comandos de SM-CLP implementan un subconjunto útil de los comandos de RACADM local. Los comandos resultan útiles para la creación de secuencias de comando pues se pueden ejecutar desde la línea de comandos de una estación de administración. La salida de los comandos se puede obtener en formatos bien definidos, incluso en XML, lo que facilita la creación de secuencias de comandos y la integración con las herramientas de informes y de administración existentes. Consulte "Equivalencias de RACADM y SM-CLP" para ver una comparación de los comandos de RACADM y SM-CLP.
IPMI	IPMI define una manera estándar en la que los subsistemas de administración incorporados, como el iDRAC6, se comunican con otros sistemas incorporados y aplicaciones de administración. Usted puede usar la interfaz Web del iDRAC6, SM-CLP o los comandos de RACADM para configurar filtros de sucesos de plataforma (PEF) de IPMI y capturas de sucesos de plataforma (PET). Los filtros de sucesos de plataforma hacen que el iDRAC6 realice acciones seleccionadas (por ejemplo, que reinicie el servidor administrado) cuando detecta una condición. Las capturas de sucesos de plataforma indican al iDRAC6 que envíe correo electrónico o alertas de IPMI cuando detecta los sucesos o condiciones especificados. También puede usar herramientas IPMI estándares como **IPMItool** e **ipmish** con iDRAC6 cuando activa la IPMI en la LAN.

Tareas de configuración

Esta sección ofrece una descripción general de las tareas de configuración de la estación de administración, el iDRAC6 y el servidor administrado. Las tareas a realizar incluyen la configuración del iDRAC6 para que se pueda usar de manera remota, la configuración de las características del iDRAC6 que usted desea usar, la instalación del sistema operativo en el servidor administrado y la instalación del software de administración en la estación de administración y el servidor administrado.

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

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

Configurar la estación de administración

Establezca una estación de administración mediante la instalación del software Dell OpenManage, un explorador Web y otras utilidades de software. Consulte "Configuración de la estación de administración".

Configurar el sistema de red de iDRAC6

Active la red de iDRAC6 y configure las direcciones IP, la máscara de red, la puerta de enlace y las direcciones DNS.

NOTA: El acceso a la configuración de iDRAC6 a través de la utilidad de configuración del iDRAC6 o CLI de RACADM local puede desactivarse con un comando RACADM (consulte "Generalidades del subcomando RACADM") o desde la interfaz gráfica para el usuario (consulte "Activación o desactivación del acceso a la configuración local").

NOTA: Si cambia la configuración de red de iDRAC6 cerrará todas las conexiones actuales de red al iDRAC6.

NOTA: La opción para configurar el servidor mediante el panel LCD *sólo* está disponible durante la configuración inicial del CMC. Una vez que el chasis está instalado, el panel LCD no se puede usar para reconfigurar el iDRAC6.

NOTA: El panel LCD se puede usar para activar DHCP para configurar la red de iDRAC6. Si desea asignar direcciones estáticas, deberá usar la utilidad de configuración del iDRAC6 o la interfaz Web del CMC.

- Panel LCD del chasis: consulte la *Guía del usuario de firmware de Dell Chasis Management Controller*.
- Utilidad de configuración del iDRAC6: consulte "Uso de la utilidad de configuración del iDRAC6"
- Interfaz Web del CMC: consulte "Configuración del sistema de red por medio de la interfaz web del CMC"
- RACADM: consulte "cfgLanNetworking"

Configurar los usuarios de iDRAC6

Configure los usuarios y permisos locales del iDRAC6. El iDRAC6 contiene una tabla de dieciséis usuarios locales en el firmware. Usted puede establecer nombres de usuarios, contraseñas y funciones para estos usuarios.

- Utilidad de configuración del iDRAC6 (sólo configura al usuario administrativo): consulte "Configuración de usuario de la LAN"
- Interfaz Web del iDRAC6: consulte "Cómo agregar y configurar usuarios de iDRAC6"
- RACADM: consulte "Incorporación de un usuario de iDRAC6"

NOTA: Cuando utiliza iDRAC6 en un entorno de Active Directory, asegúrese de que los nombres de usuarios cumplan con la convención de denominaciones de Active Directory vigente.

Configurar Active Directory

Además de los usuarios locales de iDRAC6, puede usar Microsoft® Active Directory® para autenticar los inicios de sesión de los usuarios de iDRAC6.

Para obtener más información, consulte "Uso de iDRAC6 con Microsoft Active Directory".

NOTA: Cuando utiliza iDRAC6 en un entorno de Active Directory, asegúrese de que los nombres de usuarios cumplan con la convención de denominaciones de Active Directory vigente.

Configurar la filtración de IP y el bloqueo de IP

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

- Interfaz Web del iDRAC6: consulte "Configuración de la filtración de IP y el bloqueo de IP"
- RACADM: consulte "Configuración de la filtración de IP (IP Range)" y "Configuración del bloqueo de IP"

Configurar los sucesos de plataforma

Los sucesos de plataforma ocurren cuando el iDRAC6 detecta una condición de advertencia o crítica de uno de los sensores del servidor administrado.

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

- Interfaz Web del iDRAC6: consulte "Configuración de los filtros de sucesos de plataforma (PEF)"
- RACADM: consulte "Configuración del PEF"

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

- Interfaz Web del iDRAC6: consulte "Configuración de capturas de suceso de plataforma (PET)"
- RACADM: consulte "Configuración de la PET"

Activación o desactivación del acceso a la configuración local

El acceso a los parámetros de configuración como la configuración de red y los privilegios de usuario puede desactivarse. Una vez desactivados, la configuración persiste al reiniciar. El acceso de escritura de configuración está bloqueado tanto para el programa RACADM local como para la utilidad de configuración iDRAC6 (al iniciar). El acceso web a los parámetros de configuración está libre y los datos de configuración siempre están disponibles para su visualización. Para obtener información acerca de la interfaz Web del iDRAC6, consulte "Activación o desactivación del acceso a la configuración local." Para comandos de ajuste cfgRac, consulte "cfgRacTuning."

Configurar los servicios del iDRAC6

Active o desactive los servicios de red del iDRAC6 (como Telnet, SSH y la interfaz del servidor Web) y reconfigure los puertos y otros parámetros de servicios.

- Interfaz Web del iDRAC6: consulte "Configuración de los servicios de iDRAC6"
- RACADM: consulte "Configuración de los servicios de Telnet y SSH del iDRAC6 por medio de RACADM local"

Configuración de la capa de conexión segura (SSL)

Configurar SSL para el servidor Web del iDRAC6.

- Interfaz Web del iDRAC6: consulte "Capa de conexión segura (SSL)"
- RACADM: consulte"cfgRacSecurity", "sslcsrgen", "sslcertupload", "sslcertdownload" y "sslcertview"

Configurar los medios virtuales

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

- Interfaz Web del iDRAC6: consulte "Configuración y uso de medios virtuales"
- Utilidad de configuración del iDRAC6: consulte "Configuración de medios virtuales"

Configurar una tarjeta multimedia VFlash

Instalar y configurar una tarjeta multimedia VFlash para utilizarla con iDRAC6.

- Interfaz Web del iDRAC6: consulte "Configuración de una tarjeta multimedia VFlash para utilizar con iDRAC6"

Instalación del software de servidor administrado

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

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

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

Configure el servidor administrado de modo que el iDRAC6 pueda capturar la imagen de la pantalla tras un bloqueo o falla general del sistema operativo.

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

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

NOTA: Debe contar con privilegios de administrador de configuración de chasis para definir la configuración de red de iDRAC6 desde CMC.

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

NOTA: La dirección IP de CMC se puede encontrar en la interfaz Web del iDRAC6 si se hace clic en **Sistema→ Acceso remoto→ CMC**. También puede abrir la interfaz Web de CMC a partir de esta pantalla.

Iniciar la interfaz basada en Web del iDRAC6 a partir de CMC

El CMC proporciona administración limitada de componentes individuales del chasis, como servidores. Para la administración completa de estos componentes individuales, el CMC proporciona un punto de inicio para la interfaz basada en Web del iDRAC6 del servidor.

Para iniciar iDRAC6 desde la pantalla **Servidores**:

1. Inicie sesión en la interfaz web del CMC.
2. Seleccione **Servidores** en el árbol del sistema.

   Aparece la pantalla **Estado de servidores**.
3. Haga clic en el icono **Iniciar GUI del iDRAC** para el servidor que desea administrar.

También puede abrir la interfaz Web del iDRAC6 para un solo servidor utilizando la lista de **Servidores** en el árbol del sistema.

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.

   Aparece la pantalla **Estado del servidor** para el servidor que seleccionó.
4. Haga clic en el icono **Iniciar GUI del iDRAC.**

Inicio de sesión único

Con la función de inicio de sesión único, puede abrir la interfaz Web del iDRAC6 desde el CMC sin tener que iniciar sesión por segunda vez. Las políticas de inicio de sesión único se describen a continuación

- Un usuario de CMC con **Server Administrator** configurado en **Privilegios del usuario** se conectará automáticamente con la interfaz Web del iDRAC6 mediante el inicio de sesión único. Después de iniciar sesión, se otorgan privilegios de administrador del iDRAC6. Esto sucede aunque el usuario no tenga una cuenta en iDRAC6 o si la cuenta no tiene privilegios de administrador.
- Un usuario de CMC que no tenga **Server Administrator** configurado en **User Privileges** pero con la misma cuenta en iDRAC6, se conectará

automáticamente con iDRAC6 mediante inicio de sesión único. Una vez conectado a la interfaz Web de iDRAC6, se otorgan privilegios a este usuario que fueron creados para la cuenta iDRAC6.

NOTA: En este contexto, "la misma cuenta" significa que el usuario tiene el mismo nombre de inicio de sesión y una contraseña para CMC y para iDRAC6. Un usuario que tiene el mismo nombre de inicio de sesión pero una contraseña diferente no será reconocido como un usuario válido.

- Un usuario de CMC que no tenga **Server Administrator** configurado en **Privilegios del usuario** o la misma cuenta en iDRAC6 *no* se conectará automáticamente con iDRAC6 mediante el inicio de sesión único. Este usuario será dirigido a la página de inicio de sesión de iDRAC6 al hacer clic en **Iniciar GUI del iDRAC**.

NOTA: En este caso, el sistema puede solicitar a los usuarios que se conecten con iDRAC6.

NOTA: Si se desactiva la LAN del iDRAC6 (LAN activada = No), el inicio de sesión único no estará disponible.

NOTA: Si se extrae el servidor del chasis, se cambia la dirección IP del iDRAC6 o la conexión de red del iDRAC6 tiene algún problema, al hacer clic en el icono **Iniciar GUI del iDRAC** puede aparecer una pantalla de error.

Configuración de la conexión de red de iDRAC6

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC.**
2. Haga clic en la ficha **Red/Seguridad**:

   Para activar o desactivar la comunicación en serie en la LAN:

   a. Haga clic en **Comunicación en serie en la LAN**.

      Aparecerá la pantalla **Comunicación en serie en la LAN**.

   b. Seleccione la casilla **Activar comunicación en serie en la LAN**. También puede cambiar la configuración de **Velocidad en baudios** y **Límite de nivel de privilegios del canal**.

   c. Haga clic en **Aplicar**.

   Para activar o desactivar IMPI en la LAN:

   a. Haga clic en **Red**.

      Aparecerá la pantalla **Configuración de la red**.

   b. Haga clic en **Configuración de la LAN IPMI**.

   c. Seleccione la casilla **Activar IPMI en la LAN.** También puede cambiar la configuración de **Límite de nivel de privilegios del canal** y **Clave de cifrado**.

   d. Haga clic en **Aplicar**.

   Para activar o desactivar DHCP:

   a. Haga clic en **Red**.

      Aparecerá la pantalla **Configuración de la red**.

   b. Haga clic en **Configuración de red**.

      - Para usar DHCP para la dirección IP del NIC, seleccione la casilla **Usar DHCP (para la dirección IP del NIC)**.
      - Para utilizar DHCP para obtener direcciones del servidor DNS, seleccione la casilla **Usar DHCP para obtener direcciones de servidor DNS**.

   c. Haga clic en **Aplicar**.

NOTA: Si decide no activar DHCP, debe introducir la dirección IP estática, la máscara de red y la puerta de enlace predeterminada del servidor.

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

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

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

La configuración de la función FlexAddress se realiza usando la interfaz Web de CMC. Para más información sobre la función FlexAddress y su configuración, consulte su *Guía del Usuario de Dell Chassis Management Controller Firmware versión 2.0*.

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

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

Actualización del firmware de iDRAC6

La actualización del firmware del iDRAC6 instala una nueva imagen de firmware en la memoria flash. Puede actualizar el firmware por medio de alguno de los métodos siguientes:

- El comando **load** de SM-CLP
- Interfaz Web del iDRAC6
- Dell Update Package (para Linux o Microsoft Windows)
- La utilidad de actualización del firmware del iDRAC6 de DOS
- Interfaz Web del CMC

Descarga del firmware o el paquete de actualización

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

Para actualizar el firmware del iDRAC6 por medio de la interfaz Web del iDRAC6 o de SM-CLP o para recuperar el iDRAC6 mediante la interfaz Web del CMC, descargue la imagen binaria que viene comprimida como archivo de extracción automática.

Para actualizar el firmware del iDRAC6 desde el servidor administrado, descargue el Dell Update Package (DUP) para el sistema operativo que se ejecuta en el servidor cuyo iDRAC6 va a actualizar.

Para actualizar el firmware del iDRAC6 por medio de la utilidad de actualización del firmware del iDRAC6 de DOS, descargue la utilidad de actualización y la imagen binaria, que vienen comprimidos en archivos de extracción automática.

Ejecutar la actualización del firmware

NOTA: Cuando la actualización de firmware del iDRAC6 comienza, todas las sesiones existentes en el iDRAC6 se desconectan y no se permiten nuevas sesiones hasta que el proceso de actualización haya terminado.

NOTA: Los ventiladores del chasis funcionan al 100% durante la actualización de firmware del iDRAC6. Cuando la actualización concluya, se reanudará la regulación normal de la velocidad de los ventiladores. Éste es el comportamiento normal y fue diseñado para proteger el servidor contra sobrecalentamientos durante el periodo en que no se puede enviar información del sensor al CMC.

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

Cuando usa el comando **load** de SM-CLP, coloque la imagen binaria de firmware en un directorio donde un servidor TFTP (Protocolo de transferencia de archivos trivial) pueda tenerlo a disposición del iDRAC6. Consulte "Actualización del firmware del iDRAC6 por medio de SM-CLP".

Cuando usa la interfaz Web del iDRAC6 o la interfaz Web del CMC, coloque la imagen binaria del firmware en un disco al que se pueda acceder desde la estación de administración en la que usted ejecuta la interfaz Web. Consulte "Actualización del firmware de iDRAC6".

NOTA: La interfaz Web del iDRAC6 también permite restablecer la configuración predeterminada de fábrica del iDRAC6.

Puede usar la interfaz Web del CMC o RACADM del CMC para actualizar el firmware de iDRAC6. Esta función está disponible cuando el firmware del iDRAC6 está en modo Normal y cuando está dañado. Consulte "Actualización del firmware del iDRAC6 por medio del CMC".

NOTA: Después de que el CMC actualiza el firmware del iDRAC6, el iDRAC6 genera nuevas claves SHA1 y MD5 para el certificado SSL. Como las claves son diferentes de las claves en el explorador Web abierto, todas las ventanas del explorador que están conectadas al iDRAC6 deben cerrarse después de finalizar la actualización del firmware. Si las ventanas del explorador no se cierran, se verá un mensaje de error **Certificado inválido.**

NOTA: Si está realizando una reversión de su firmware iDRAC6 a una versión anterior, debe eliminar el complemento existente del explorador Internet Explorer ActiveX® de cualquier estación de administración (Management Station) basada en Windows para permitir que el firmware instale una versión compatible del complemento ActiveX. Consulte "Eliminación del complemento ActiveX" para obtener más información.

Eliminación del complemento ActiveX

Debe eliminar el complemento existente del explorador Internet Explorer ActiveX de cualquier Management Station basada en Windows para permitir que el firmware instale una versión compatible del complemento ActiveX.

Para eliminar el complemento ActiveX en Internet Explorer 6:

1. Vaya a **C:\WINDOWS\Downloaded Program Files**.
2. Elimine el archivo **DELL IDRAC 11G AVCView**.

Para eliminar el complemento ActiveX en Internet Explorer 7:

1. Abra Internet Explorer 7.
2. De ser necesario, presione la tecla <Alt> para ver la barra de menús.

3. Haga clic en **Herramientas**→ **Administrar complementos**→ **Habilitar o deshabilitar complementos**.
4. En la ventana **Administrar complementos**, seleccione **Controles ActiveX descargados (32 bits)** en el menú desplegable **Mostrar**.
5. En la lista **Habilitado**, haga clic en **DELL IDRAC 11G AVCView**, y luego haga clic en el botón **Eliminar** en la sección **Eliminar ActiveX**.
6. Haga clic en **Aceptar**.

Uso de la interfaz Web del iDRAC6

PRECAUCIÓN: Si el firmware del iDRAC6 se daña, como puede suceder cuando el progreso de la actualización del firmware del iDRAC6 se interrumpe antes de terminar, puede recuperar el iDRAC6 por medio de la interfaz Web del iDRAC6.

NOTA: De manera predeterminada, la actualización del firmware retendrá la configuración actual del iDRAC6. Durante el proceso de actualización, tiene la opción de restablecer la configuración predeterminada de fábrica del iDRAC6. Si establece la configuración predeterminada de fábrica, el acceso a la red externa se desactivará cuando la actualización termine. Debe activar y configurar la red por medio de la utilidad de configuración del iDRAC6.

1. Inicie la interfaz Web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**.
3. Haga clic en la ficha **Actualizar**.

   Aparecerá la pantalla **Actualización del firmware**.

   NOTA: Para actualizar el firmware, el iDRAC6 debe estar en el modo de actualización. Cuando se encuentre en este modo, el iDRAC6 se restablecerá automáticamente, aun cuando usted cancele el proceso de actualización.

4. En la sección **Cargar (Paso 1 de 4)**, haga clic en **Examinar para ubicar** la imagen del firmware que descargó. También puede escribir la ruta en el campo de texto. Por ejemplo:

   `C:\Updates\V2.0\<image_name>`.

   El nombre predeterminado de la imagen del firmware es **firmimg.imc**.

5. Haga clic en **Cargar**.

   El archivo se cargará en el iDRAC6. This may take several minutes to complete.

   NOTA: Durante el proceso de carga, puede anular el proceso de actualización del firmware al hacer clic en **Cancelar**. Al hacer clic en **Cancelar,** el iDRAC6 se restablecerá al modo de operación normal.

   Una vez que la carga ha finalizado, aparece la pantalla **Actualización del firmware: Validación (página 2 de 4)**.

   - Cuando el archivo de imagen se cargue exitosamente y pase todas las revisiones de verificación, aparecerá un mensaje indicando que la imagen del firmware ha sido verificada.
   - Cuando la imagen no se cargue correctamente o cuando no pase las revisiones de verificación, la actualización del firmware regresará a la pantalla **Actualización del firmware**. Puede intentar actualizar el iDRAC6 nuevamente o hacer clic en **Cancelar** para restablecer el iDRAC6 al modo de operación normal.

   NOTA: Si deselecciona la casilla Conservar configuración, el iDRAC6 restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está desactivada y usted no puede iniciar sesión en la interfaz Web del iDRAC6. Debe reconfigurar los valores de la LAN por medio de la utilidad de configuración del iDRAC6 durante la POST del BIOS.

6. De manera predeterminada, la casilla **Conservar configuración** está activada (seleccionada) para conservar los valores actuales en el iDRAC6 después de una actualización. Si no desea conservar los valores, deseleccione la casilla **Conservar configuración**.
7. Haga clic en **Comenzar la actualización** para iniciar el proceso de actualización. No interrumpa el proceso de actualización.
8. En la ventana **Actualización del firmware: Actualización (página 3 de 4)**, verá el estado de la actualización. El progreso de la operación de actualización de firmware, expresado en porcentaje, aparecerá en la columna **Progreso**.
9. Una vez que la actualización del firmware concluya, aparecerá la ventana **Actualización del firmware: Resultados de la actualización (página 4 de 4)** y el iDRAC6 se restablecerá automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana nueva de explorador.

Uso de la utilidad de actualización de DOS

Para actualizar el firmware del iDRAC6 por medio de la utilidad de actualización de DOS, inicie el servidor administrado en DOS y ejecute el comando **idrac16d**. La sintaxis del comando es:

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

Cuando se ejecuta sin agregar opciones, el comando **idrac16d** actualiza el firmware del iDRAC6 con el archivo de imagen de firmware **firmimg.imc** en el directorio actual.

Las opciones son las siguientes:

- `-f`: fuerza la actualización. La opción `-f` se puede usar para *degradar* el firmware a una imagen anterior.
- `-i=<nombre de archivo>`: especifica el nombre del archivo que contiene la imagen de firmware. Esta opción es necesaria cuando el nombre de archivo predeterminado del firmware, **firmimg.imc**, ha sido cambiado.
- `-l=<archivo_de_registro>`: registra la salida de la actividad de actualización. Esta opción se usa para depuración.

NOTA: Si usted introduce argumentos incorrectamente con el comando **idrac16d** o añade la opción `-h`, tal vez note una opción adicional, `-nopresconfig` en el mensaje de salida sobre su uso. Esta opción se usa para actualizar el firmware sin conservar la información de configuración. **No** debe utilizar esta opción a menos que así se lo indique expresamente un representante del servicio de asistencia de Dell, pues se *eliminará* toda la información existente sobre la configuración del iDRAC6, como las direcciones IP, los usuarios y las contraseñas.

Verificación de la firma digital

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

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

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

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

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

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

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

   a. Introduzca el comando siguiente:

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

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

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

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

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

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


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

      Your decision?

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

      1 = no sé o me abstengo
      2 = no confío en él
      3 = confío en él con reservas
      4 = confío en él
      5 = confío en él plenamente
      m = regresar al menú principal

      ¿Cuál es su decisión?)
      ```

   d. Introduzca 5, y luego presione <Entrar>. Aparecerá la siguiente petición:

      ```
      Do you really want to set this key to ultimate trust? (y/N)
      (¿Realmente desea otorgar plena confianza a esta clave? [y/N])
      ```

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

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

Debe importar y validar la clave pública sólo una vez.

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

NOTA: Cada paquete de actualización de Linux tiene un archivo de firma independiente, que aparece en la misma página Web que el paquete de actualización. Usted necesita el paquete de actualización y el archivo de firma relacionado para la verificación. De manera predeterminada, el archivo de firma tiene el mismo nombre que el archivo del DUP, con la extensión **.sign**. Por ejemplo, la imagen del firmware del iDRAC6 tiene un archivo **.sign** asociado (**IDRAC_FRMW_LX_2.0.BIN.sign**), que se incluye en el archivo de extracción automática con la imagen del firmware (**IDRAC_FRMW_LX_2.0.BIN**). Para descargar los archivos, haga clic con el botón derecho del mouse en el vínculo de descarga y use la opción **Guardar destino como...** del archivo.

5. Verifique el paquete de actualización:

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

El ejemplo siguiente ilustra los pasos a seguir para verificar un paquete de actualización del Dell PowerEdge™ M610 iDRAC:

1. Descargue los dos archivos siguientes de **support.dell.com**:
   - IDRAC_FRMW_LX_2.0.BIN.sign
   - IDRAC_FRMW_LX_2.0.BIN

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

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

Aparecerá el siguiente mensaje de salida:

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

(gpg: la clave 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" no se modificó
gpg: Número total procesado: 1
gpg: sin modificar: 1)
```

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

a. Introduzca el comando siguiente:

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

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

```
fpr
trust
```

c. Escriba 5 y luego presione <Entrar> para elegir `I trust ultimately (confío plenamente)` en el menú.

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

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

Esto completa la validación de la clave pública de Dell.

4. Verifique la firma digital del paquete PowerEdge M610 iDRAC mediante la ejecución del comando siguiente:

```
gpg --verify IDRAC_FRMW_LX_2.0.BIN.sign IDRAC_FRMW_LX_2.0.BIN
```

Aparecerá el siguiente mensaje de salida:

```
gpg: Signature made Fri Jul 11 15:03:47 2008 CDT using DSA key ID 23B66A9D
gpg: Good signature from "Dell, Inc. (Product Group) <linux-security@dell.com>"

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

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

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

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

Limpiar el caché del explorador

Para poder usar las funciones del último iDRAC6, deberá limpiar el caché del explorador para eliminar cualquier página *antigua* que podría estar guardada en el sistema.

Internet Explorer 6

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

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

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

Internet Explorer 7

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

   Aparece la ventana **Opciones de Internet**.
3. Haga clic en la ficha **General**.
4. En **Historial de exploración,** haga clic en **Eliminar...**.

   Ahora aparece la ventana **Eliminar archivos**.
5. Haga clic en **Eliminar archivos** al lado de **Archivos temporales de Internet**.
6. Haga clic en **Cerrar**, y después en **Aceptar** para salir de la ventana **Opciones de Internet**.

Firefox

1. Inicie Firefox.
2. Haga clic en **Editar**→ **Preferencias**.
3. Haga clic en la ficha **Privacidad**.
4. Haga clic en **Limpiar la caché ahora**.
5. Haga clic en **Cerrar**.

Actualización del paquete de reparación de USC

Consulte la *Guía del usuario de Dell Unified Server Configurator* para obtener información sobre la actualización del paquete de reparación de USC desde la interfaz Web del iDRAC6.

Configuración del iDRAC6 para usarlo con IT Assistant

Dell OpenManage IT Assistant puede descubrir dispositivos administrados que cumplan con las versiones 1 y 2c del Protocolo simple de administración de red (SNMP) y la Interfaz de administración de plataforma inteligente (IPMI) versión 2.0.

El iDRAC6 cumple con IPMI versión 2.0. En esta sección se describen los pasos necesarios para configurar iDRAC6 para el descubrimiento y la supervisión a través de IT Assistant. Existen dos formas de llevar a cabo este procedimiento: mediante la utilidad de configuración del iDRAC6 y por medio de la interfaz gráfica Web del iDRAC6.

Uso de la utilidad de configuración del iDRAC6 para activar las funciones de descubrimiento y supervisión

Para configurar el iDRAC6 para el descubrimiento de IPMI y el envío de capturas de alerta por medio de la utilidad de configuración del iDRAC6, reinicie el servidor administrado (blade) y controle el proceso de encendido por medio de iKVM y un teclado de consola y supervisión remota o bien una conexión en serie en la LAN (SOL). Cuando aparezca la indicación `Press <Ctrl-E> for Remote Access Setup (Presione <Ctrl-E> para configurar el acceso remoto)`, oprima `<Ctrl><E>`.

Cuando aparezca la pantalla **Utilidad de configuración del iDRAC**, utilice las teclas de flechas para desplazarse hacia abajo.

1. Active la opción **IPMI en la LAN**.
2. Introduzca la **Clave de cifrado RMCP+** del sitio, si utiliza una.

   NOTA: Consulte al administrador de red o al director de IT para analizar la posibilidad de implementar esta opción, ya que agrega una valiosa protección de la seguridad y debe instalarse en todo el sitio para que funcione correctamente.

3. En la sección **Parámetros de LAN**, presione <Entrar> para ingresar a la pantalla secundaria. Utilice las teclas de flecha hacia arriba y hacia abajo para recorrer la pantalla.
4. Con la barra espaciadora, **active** la opción **Alerta de LAN activada**.
5. Introduzca la dirección IP de su estación de administración en **Destino de alerta 1**.
6. En **Nombre de iDRAC6**, introduzca un nombre que cumpla con la convención utilizada en el centro de datos. El nombre predeterminado es `iDRAC6-{Etiqueta de servicio}`.

Para salir de la Utilidad de configuración del iDRAC6 presione <Esc>, <Esc> y luego <Entrar> para guardar los cambios. El servidor se iniciará en el modo de operación normal e IT Assistant lo detectará durante la próxima pasada de descubrimiento programada.

Uso de la interfaz Web del iDRAC6 para activar las funciones de descubrimiento y supervisión

El descubrimiento de IPMI también puede activarse a través de la interfaz Web remota:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz basada en Web del iDRAC6 con el nombre de usuario y la contraseña con derechos de administrador.
3. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**.
4. Haga clic en la ficha **Red/Seguridad**.

   Aparecerá la pantalla **Configuración de red**.

5. Haga clic en **Configuración de la LAN IPMI**.
6. Asegúrese de que la casilla **Activar IPMI en la LAN** esté seleccionada.
7. Seleccione **Administrador** en el menú desplegable **Privilegios de nivel de canal**.
8. Introduzca la **Clave de cifrado** RMCP+ del sitio, si utiliza una.
9. Haga clic en **Aplicar** si realizó cambios en esta pantalla.
10. Seleccione **Sistema** en el árbol del sistema.
11. Haga clic en la ficha **Administración de alertas** y después haga clic en **Sucesos de plataforma**.

    Aparecerá la pantalla **Sucesos de plataforma** con una lista de sucesos para los cuales puede configurar iDRAC6 a fin de generar alertas por correo electrónico.

12. Active la generación de alertas para uno o más sucesos al seleccionar la casilla en la columna **Generar alertas**.

13. Haga clic en **Aplicar** si realizó cambios en esta pantalla.

14. Haga clic en **Configuración de captura**.

    Aparecerá la pantalla **Destinos de alertas de sucesos de plataforma**.

15. En el primer campo disponible **Dirección IP de destino** de la sección **Lista de destinos de iPv4**, seleccione la casilla **Activado**, y luego escriba la dirección IP de su estación de administración.

16. Haga clic en **Aplicar** si realizó cambios en esta pantalla.

Ahora puede enviar una captura de prueba al hacer clic en el vínculo **Enviar** en la columna **Captura de prueba**.

Por motivos de seguridad, Dell recomienda especialmente crear un usuario separado para los comandos de IPMI con un nombre de usuario, privilegios de IPMI en la LAN y contraseña propios:

1. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**.

2. Haga clic en la ficha **Seguridad de red** y luego haga clic en **Usuarios**.

   Aparecerá la pantalla **Usuarios** con una lista de todos los usuarios (definidos o no definidos).

3. Haga clic en la **Identificación de usuario** de un usuario no definido.

   Aparecerá la pantalla **Configuración de usuario** para la identificación de usuario que seleccionó.

4. Seleccione la casilla **Activar usuario**, y luego escriba el nombre de usuario y la contraseña.

5. En la sección **Privilegios de LAN de IMPI**, asegúrese de que **Privilegio máximo permitido de usuario de LAN** esté definido como **Administrador**.

6. Establezca los privilegios de usuario.

7. Haga clic en **Aplicar** para guardar la configuración de nuevos usuarios.

Uso de IT Assistant para ver el estado y los sucesos del iDRAC6

Después de completar la configuración de descubrimiento, los dispositivos del iDRAC6 aparecerán en la categoría **Servidores** de la pantalla **Detalles de dispositivos ITA**, y su información podrá visualizarse al hacer clic en el nombre del iDRAC6. Esto difiere de los sistemas DRAC5, en los que la tarjeta de administración aparece en el grupo de RAC. Esto se debe al hecho de que el iDRAC6 utiliza el descubrimiento de IPMI y no SNMP.

Las capturas de advertencias y errores de iDRAC6 ahora pueden visualizarse en el **Registro de alertas** principal de IT Assistant. Aunque aparecen en la categoría **Desconocido**, la descripción y gravedad de las capturas se indican con exactitud.

Para obtener más información sobre el uso de IT Assistant para administrar el centro de datos, consulte la *Guía del usuario de Dell OpenManage IT Assistant*.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la estación de administración

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Una estación de administración es un equipo que se usa para supervisar y administrar los servidores PowerEdge y otros módulos en el chasis. Esta sección describe la instalación del software y las tareas de configuración que preparan una estación de administración para trabajar con iDRAC6 Enterprise. Antes de comenzar a configurar el iDRAC6, siga los procedimientos de esta sección para asegurarse de haber instalado y configurado las herramientas que necesitará.

Pasos de configuración de la estación de administración

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

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

Requisitos de la red de la estación de administración

Para tener acceso al iDRAC6, la estación de administración debe estar en la misma red que el puerto de conexión RJ45 del CMC que está etiquetado como "GB1". Es posible aislar la red del CMC de la red en la que se encuentra el servidor administrado, de modo que la estación de administración pueda tener acceso por LAN al iDRAC6 pero no al servidor administrado.

Por medio de la función de redirección de consola del iDRAC6 (consulte "Configuración y uso de la comunicación en serie en la LAN"), es posible acceder a la consola del servidor administrado aun sin acceso de red a los puertos del servidor. Usted también puede ejecutar varias funciones de administración en el servidor administrado, como por ejemplo el reinicio del equipo, mediante los servicios del iDRAC6. Sin embargo, para tener acceso a red y a los servicios de aplicación que se encuentran en el servidor administrado, es posible que necesite tener una tarjeta adicional de interfaz de red en el equipo de administración.

Configuración de un explorador de web admitido

Las secciones siguientes contienen instrucciones para configurar los exploradores Web admitidos para su uso con la interfaz Web del iDRAC6. Para ver una lista de los exploradores de web admitidos, consulte "Exploradores web admitidos".

Abrir el explorador web

La interfaz Web del iDRAC6 está diseñada para verse en un explorador Web compatible con una resolución de pantalla mínima de 800 píxeles de ancho por 600 de alto. Para poder visualizar la interfaz y acceder a todas las funciones, asegúrese de que su resolución esté configurada al menos en 800 por 600 pixeles y/o cambie el tamaño de su explorador, según sea necesario.

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

Configuración del explorador web para conectarse a la interfaz web

Si se conecta a la interfaz Web del iDRAC6 desde una estación de administración conectada a Internet mediante un servidor proxy, debe configurar el explorador Web para que acceda a Internet desde este servidor.

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

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

   Aparece la ventana **Opciones de Internet**.
3. Seleccione **Herramientas**→ **Opciones de Internet**→ **Seguridad**→ **Red local**.
4. Haga clic en **Nivel personalizado**.
5. Seleccione la opción **Medio bajo** en el menú desplegable y luego haga clic en **Restablecer**. Haga clic en **Aceptar** para confirmar. Deberá hacer clic en este botón para regresar al cuadro de diálogo **Nivel personalizado**.
6. Desplácese hacia abajo hasta la sección de controles y complementos de ActiveX y verifique cada configuración, pues las distintas versiones de IE muestran diferentes valores para el estado **Medio bajo**:
   - Preguntar automáticamente si se debe usar un control ActiveX: Habilitar
   - Comportamiento de binarios y de scripts: Habilitar
   - Descargar los controles ActiveX firmados: Preguntar
   - Inicializar y generar scripts de los controles ActiveX no marcados como seguros: Preguntar
   - Ejecutar controles y complementos de ActiveX: Habilitar
   - Generar scripts de los controles ActiveX marcados como seguros para scripting: Habilitar

   En la sección de **Descargas**:
   - Preguntar automáticamente si se debe descargar un archivo: Habilitar
   - Descarga de archivos: Habilitar
   - Descarga de fuentes: Habilitar

   En la sección **Miscelánea**:
   - Permitir META-REFRESH: Habilitar
   - Permitir la ejecución de scripts en el control del explorador web de Internet Explorer: Habilitar
   - Permitir que se abran ventanas generadas por scripts sin ninguna restricción de tamaño o posición: Habilitar
   - No pedir que se seleccione un certificado de cliente cuando exista sólo uno o cuando no exista ninguno: Habilitar
   - Ejecutar programas y archivos en IFRAME: Habilitar
   - Abrir archivos basándose en el contenido, no en la extensión de archivo: Habilitar
   - Permisos de canal de software: Seguridad baja
   - Enviar los datos no cifrados del formulario: Habilitar
   - Usar el bloqueador de elementos emergentes: Deshabilitar

   En la sección **Automatización**:
   - Active scripting: Habilitar
   - Permitir operaciones de pegado por medio de una secuencia de comandos: Habilitar
   - Scripting de applets de Java: Habilitar
7. Seleccione **Herramientas**→ **Opciones de Internet**→ **Opciones avanzadas**.
8. Verifique que las siguientes opciones se encuentren seleccionadas o deseleccionadas, según corresponda:

   En la sección **Examinar**:
   - Enviar direcciones URL en UTF-8: seleccionada
   - Deshabilitar la depuración de scripts (Internet Explorer): seleccionada
   - Deshabilitar la depuración de scripts (otros): seleccionada
   - Mostrar una notificación sobre cada error de script: deseleccionada
   - Habilitar la instalación a petición (otros): seleccionada
   - Habilitar transiciones de página: seleccionada
   - Habilitar extensiones de explorador de terceros: seleccionada
   - Iniciar accesos directos en ventanas ya abiertas: deseleccionada

En la sección **Configuración de HTTP 1.1**:

- Usar HTTP 1.1: seleccionada
- Usar HTTP 1.1 en conexiones proxy: seleccionada

En la sección **Java (Sun)**:

- Utilizar JRE 1.6.x_yz: seleccionada (opcional; la versión puede diferir)

En la sección **Multimedia**:

- Habilitar Cambio automático del tamaño de imágenes: seleccionada
- Activar animaciones en páginas Web: seleccionada
- Mostrar videos en páginas Web: seleccionada
- Mostrar imágenes: seleccionada

En la sección **Seguridad**:

- Comprobar si se revocó el certificado del editor: deseleccionada
- Comprobar si existen firmas en los programas descargados: deseleccionada
- Comprobar si existen firmas en los programas descargados: seleccionada
- Usar SSL 2.0: deseleccionada
- Usar SSL 3.0: seleccionada
- Usar TLS 1.0: seleccionada
- Advertir sobre certificados de sitios no válidos: seleccionada
- Advertir si se cambia entre un modo seguro y un modo no seguro: seleccionada
- Advertir si se redirige el envío de formularios: seleccionada

NOTA: Si decide cambiar alguna de las opciones anteriores, Dell recomienda asegurarse de aprender y comprender las consecuencias de dicha acción. Por ejemplo, si opta por bloquear los mensajes emergentes, ciertas partes de la interfaz Web del iDRAC6 no funcionarán correctamente.

9. Haga clic en **Aplicar** y después en **Aceptar**.
10. Haga clic en la ficha **Conexiones**.
11. En **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.
12. Si la casilla **Usar servidor proxy** está seleccionada, seleccione la casilla **No usar servidor proxy para direcciones locales**.
13. Haga clic dos veces en **Aceptar**.
14. Cierre y reinicie el explorador para asegurarse de que todos los cambios tengan efecto.

Cómo agregar el iDRAC6 a la lista de dominios de confianza

Al acceder a la interfaz Web de iDRAC6 a través del explorador Web, es posible que se le pida que agregue la dirección IP de iDRAC6 a la lista de dominios de confianza, si dicha dirección IP no figura en la lista. Al terminar, haga clic en **Actualizar** o vuelva a iniciar el explorador Web para establecer una conexión con la interfaz Web de iDRAC6.

Cómo ver las versiones traducidas de la interfaz web

La interfaz Web del iDRAC6 es compatible con los siguientes idiomas de sistema operativo:

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

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

La interfaz Web del iDRAC6 está diseñada para funcionar con teclados localizados para las variantes de idiomas específicos mencionados anteriormente. Algunas funciones de la interfaz Web del iDRAC6, como la Redirección de consola, pueden requerir pasos adicionales para aceptar algunas funciones/letras.

Para obtener más detalles sobre cómo usar su teclado localizado en estos casos, consulte "Uso de Video Viewer". El uso de otros teclados no es compatible y puede causar problemas inesperados.

Internet Explorer 6.0 (Windows)

Para ver una versión traducida de la interfaz Web de iDRAC6 en Internet Explorer, realice los pasos que se indican a continuación:

1. Haga clic en el menú **Herramientas** y seleccione **Opciones de Internet**.
2. En la ventana **Opciones de Internet**, haga clic en **Idiomas**.
3. En la ventana **Preferencias de idioma** haga clic en **Agregar**.
4. En la ventana **Agregar idioma**, seleccione un idioma compatible.

   Para seleccionar más de un idioma, presione <Ctrl>.
5. Seleccione el idioma de su preferencia y haga clic en **Subir** para subir el idioma a la parte superior de la lista.
6. En la ventana **Preferencias de idioma**, haga clic en **Aceptar**.
7. Haga clic en **Aceptar**.

Firefox 2.0 (Linux o Windows)

Para ver una versión traducida de la interfaz Web de iDRAC6 en Firefox 2.0, realice los pasos que se indican a continuación:

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

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

Cómo establecer la configuración regional en Linux

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

Para establecer el conjunto de caracteres en un cliente Linux con una interfaz gráfica de usuario en chino simplificado:

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

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

3. Si los valores incluyen zh_CN.UTF-8, no será necesario hacer cambios. Si los valores no incluyen zh_CN.UTF-8, vaya al paso 4.

4. Modifique el archivo **/etc/sysconfig/i18n** con un editor de textos.

5. En el archivo, aplique los cambios siguientes:

   Anotación actual:

   ```
   LANG="zh_CN.GB18030"
   SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```

   Anotación actualizada:

   ```
   LANG="zh_CN.UTF-8"
   SUPPORTED="zh_CN.UTF-8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```

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

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

Desactivación de la función de lista blanca en Firefox

Firefox tiene una función de seguridad de "lista blanca" que requiere permiso del usuario para instalar complementos para cada sitio distinto que aloje un complemento. Cuando está activada, la función de lista blanca ("whitelist") requiere que se instale un visor de redirección de consola por cada iDRAC6 que usted visite, aunque las versiones del visor sean idénticas.

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

1. Abra una ventana del explorador de web Firefox.

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

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

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

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

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

Instalación de Java Runtime Environment (JRE)

NOTA: Si usa el explorador Internet Explorer, se ofrece un control ActiveX para el visor de consola. También puede usar el visor de consola de Java con Internet Explorer si instala JRE y configura el visor de consola en la interfaz Web del iDRAC6 antes de ejecutar el visor. Consulte "Configuración de la redirección de consola y Medios virtuales en la interfaz web del iDRAC6" para obtener más información.

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

Si usa el explorador Firefox deberá instalar JRE (o un paquete de desarrollo de Java [JDK]) para usar la función de redirección de consola. El visor de consola es una aplicación de Java que se descarga en la estación de administración desde la interfaz Web del iDRAC6 y después se ejecuta con Java Web Start en la estación de administración.

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

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

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

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

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

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

Instalación de clientes Telnet o SSH

De manera predeterminada, el servicio Telnet del iDRAC6 está desactivado y el servicio SSH está activado. Como Telnet es un protocolo inseguro, sólo debe

usarse cuando no se puede instalar un cliente SSH o la conexión de red tiene otro tipo de seguridad.

NOTA: Sólo puede haber una conexión Telnet o SSH activa con el iDRAC6 a la vez. Cuando haya una conexión activa, se rechazarán los demás intentos de conexión.

Telnet con iDRAC6

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

Si la estación de administración está ejecutando Windows XP SP1 o Windows 2003, es posible que tenga un problema con los caracteres en una sesión Telnet de iDRAC6. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión en el que la tecla <Entrar> no responde y no aparece la petición de contraseña.

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

NOTA: La actualización sólo es necesaria para Windows XP SP1 y Windows 2003. En Windows XP SP2 se resolvió el problema.

Configuración de la tecla de retroceso para las sesiones de Telnet

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

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

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

   `telnet`

   Si está ejecutando una sesión de Telnet, presione <Ctrl><]>.
3. En el indicador, introduzca:

   `set bsasdel`

   Aparece el mensaje siguiente:

   `Backspace will be sent as delete. (El retroceso se procesará como eliminación.)`

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

1. Abra un shell y escriba:

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

   `telnet`

SSH con iDRAC6

Secure Shell (SSH) es una conexión de línea de comandos con las mismas capacidades que una sesión Telnet, pero con negociación de sesión y cifrado para mejorar la seguridad. El iDRAC6 admite la versión 2 de SSH con autentificación de contraseña. SSH está activado en el iDRAC6 de manera predeterminada.

Se puede usar PuTTY (en Windows) u OpenSSH (en Linux) en una estación de administración para conectarse al iDRAC6 del servidor administrado. Cuando se presenta un error durante el procedimiento de inicio de sesión, el cliente de **ssh** envía un mensaje de error. El texto del mensaje está en función del cliente y no es controlado por el iDRAC6.

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

Sólo se admite una sesión de Telnet o de SSH en un momento dado. El tiempo de espera de la sesión lo controla la propiedad `cfgSsnMgtSshIdleTimeout`, según se describe en "Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6".

La implementación de SSH del iDRAC6 admite varios esquemas de criptografía, según se muestra en la tabla 3-1.

NOTA: No se admite SSHv1.

Tabla 3-1. Esquemas de criptografía

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

Instalación de un servidor TFTP

NOTA: Si usa únicamente la interfaz Web del iDRAC6 para transferir certificados de SSL y cargar nuevo firmware al iDRAC6, no necesita un servidor TFTP.

El Protocolo de transferencia de archivos trivial (TFTP) es una forma simplificada del Protocolo de transferencia de archivos (FTP). Se usa con las interfaces de línea de comandos de SM-CLP y RACADM para intercambiar archivos con el iDRAC6.

Las únicas ocasiones en las que necesita copiar archivos desde o en el iDRAC6 surgen cuando actualiza el firmware del iDRAC6 o cuando instala certificados en el iDRAC6. Si decide usar SM-CLP o RACADM cuando realice estas tareas, deberá tener un servidor TFTP funcionando en un equipo al que el iDRAC6 pueda tener acceso por medio del número de IP o del nombre DNS.

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

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

Instalación de Dell OpenManage IT Assistant

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

- DVD *Dell Systems Management Tools and Documentation*
- Sitio web de asistencia Dell Support y archivos léame: consulte los archivos léame y el sitio web de asistencia Dell Support en la dirección **support.dell.com** para ver la información más reciente de los productos Dell.

Utilice el DVD *Dell Systems Management Tools and Documentation* para instalar el software de consola de administración, incluso Dell OpenManage IT Assistant, en la estación de administración Para obtener instrucciones sobre cómo instalar este software, consulte la *Guía de instalación rápida del software Dell OpenManage*.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del servidor administrado

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

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

Instalación del software en el servidor administrado

El software de administración de Dell incluye los siguientes componentes:

- CLI de RACADM local: permite configurar y administrar el iDRAC6 desde el servidor administrado. Es una herramienta potente tareas de configuración y administración de secuencias de comando.
- Server Administrator: se requiere que éste use la función de pantalla de último bloqueo del iDRAC6.
- Server Administrator Instrumentation Service: proporciona acceso a información detallada sobre fallas y rendimiento recopilada por agentes de administración de sistemas estándar de la industria, y permite la administración remota de sistemas supervisados, incluso acciones de apagado, inicio y seguridad.
- Server Administration Storage Management Service: brinda información sobre administración de almacenamiento en una vista gráfica integrada.
- Registros de Server Administrator: muestran registros de los comandos recibidos o enviados por el sistema, los sucesos de hardware supervisados, los sucesos de la POST y las alertas del sistema. Los registros se pueden ver en la página de inicio, imprimir o guardar como informes y enviarse por correo electrónico a un contacto de servicio designado.

Utilice el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de administración de sistemas Dell) para instalar Server Administrator. Para obtener instrucciones sobre cómo instalar este software, consulte la *Guía de instalación rápida*.

Configuración del servidor administrado para capturar la pantalla de último bloqueo

El iDRAC6 puede capturar la pantalla del último bloqueo para que usted pueda verla en la interfaz web a fin de ayudar a solucionar la causa del bloqueo del servidor administrado. Siga estos pasos para activar la función de pantalla del último bloqueo.

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

2. Si ejecuta Windows, asegúrese de que la función **Reinicio automático** esté deseleccionada en la **Configuración de Inicio y recuperación de Windows**. Consulte "Desactivación de la opción de reinicio automático de Windows".

3. Active la **Pantalla del último bloqueo** (desactivada de manera predeterminada) en la interfaz web del iDRAC6.

   Para activar la **Pantalla del último bloqueo** en la interfaz web del iDRAC6, haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**→ **Servicios**, y luego haga clic en la casilla **Activar** que se encuentra bajo el encabezado Configuración del agente de recuperación automatizada del sistema.

   Para activar la Pantalla del último bloqueo por medio de RACADM local, abra un indicador de comandos en el servidor administrado y escriba el siguiente comando:

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

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

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

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

Desactivación de la opción de reinicio automático de Windows

Para asegurarse de que el iDRAC6 pueda capturar la pantalla del último bloqueo, desactive la opción **Reinicio automático** en los servidores administrados que ejecutan Windows Server o Windows Vista.

1. Abra el **Panel de control** de Windows y haga doble clic en el icono **Sistema**.

2. Haga clic en la ficha **Opciones avanzadas**.
3. En **Inicio y recuperación**, haga clic en **Configuración**.
4. Deseleccione la casilla **Reiniciar automáticamente**.
5. Haga clic dos veces en **Aceptar**.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del iDRAC6 Enterprise por medio de la interfaz Web

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

El iDRAC6 ofrece una interfaz Web que permite configurar las propiedades y usuarios del iDRAC6, realizar tareas de administración remota y solucionar problemas de un sistema (administrado) remoto. Para la administración diaria de sistemas, use la interfaz Web de iDRAC6. Este capítulo proporciona información sobre cómo realizar tareas comunes de administración de sistemas con la interfaz Web de iDRAC6 y proporciona vínculos con información relacionada.

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

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

Los comandos de SM-CLP se ejecutan en un shell al que se puede tener acceso de manera remota con una conexión Telnet o SSH. Para obtener más información sobre SM-CLP, consulte "Uso de la interfaz de línea de comandos de SM-CLP de iDRAC6 ".

Acceso a la interfaz web

Para acceder a la interfaz Web de iDRAC6, realice los pasos que se indican a continuación:

1. Abra una ventana de un explorador web compatible.

   Consulte "Exploradores web admitidos" para obtener más información.

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

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

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

   donde *dirección_IP_de_iDRAC6* es la dirección IP de iDRAC y *número_de_puerto* es el número del puerto HTTPS.

   Aparecerá la ventana **Inicio de sesión** del iDRAC6.

Conexión

Puede iniciar sesión como usuario del iDRAC6 o como usuario de Microsoft® Active Directory®. El nombre predeterminado y la contraseña son **root** y **calvin**, respectivamente.

Para que pueda iniciar sesión en el iDRAC6, el administrador debe haberle otorgado privilegio de **Inicio de sesión en el iDRAC**.

Para conectar, realice los pasos siguientes:

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

   - Su nombre de usuario de iDRAC6.

     En el nombre de usuario para los usuarios locales se distingue entre mayúsculas y minúsculas. Algunos ejemplos son `root`, `usuario_de_TI` o `juan_perez`.

   - Su nombre de usuario de Active Directory.

     Puede usar cualquiera de los siguientes formatos para los nombres de Active Directory: <*dominio*>\<*nombre_de_usuario*>, <*dominio*>/<*nombre_de_usuario*> o <*usuario*>@<*dominio*>. En ellos no se distingue entre mayúsculas y minúsculas. Algunos ejemplos son `dell.com\juan_perez`, o `JUAN_PEREZ@DELL.COM`. Como alternativa, puede escribir el dominio en el campo **Dominio**.

2. En el campo **Contraseña**, introduzca la contraseña de usuario del iDRAC6 o la contraseña de usuario de Active Directory. Las contraseñas distinguen entre mayúsculas y minúsculas.

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

Desconexión

1. En la esquina superior derecha de la ventana principal, haga clic en **Desconectar** para cerrar la sesión.
2. Cierre la ventana del explorador.

NOTA: El botón **Desconectar** no aparecerá a menos que usted haya iniciado sesión.

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

NOTA: Si se cierra la interfaz Web de iDRAC6 en Internet Explorer mediante el botón para cerrar ("x"), que se encuentra en la esquina superior derecha de la ventana, podría generarse un error de aplicación. Para resolver este problema, descargue la actualización de seguridad acumulativa más reciente para Internet Explorer desde el sitio Web de asistencia de Microsoft, en **support.microsoft.com**.

Uso de varias fichas y ventanas del explorador

Las distintas versiones de exploradores Web muestran diferentes comportamientos al abrir nuevas fichas y ventanas. Cada ventana es una nueva sesión, mientras que cada ficha no lo es. Microsoft Internet Explorer 6 no admite fichas; por lo tanto, cada ventana que se abre en el explorador es una sesión nueva de la interfaz Web de iDRAC6. Internet Explorer 7 tiene la opción de abrir fichas así como también ventanas. Cada ficha hereda las características de la ficha abierta más recientemente. Por ejemplo, si un usuario inicia sesión con privilegios de usuario avanzado en una ficha y después inicia sesión como Administrador en otra ficha, ambas fichas abiertas tendrán privilegios de administrador. Al cerrar una ficha finalizan todas las fichas de interfaz Web de iDRAC6.

La acción de las fichas en Firefox 2 es igual que en Internet Explorer 7: las nuevas fichas inician nuevas sesiones. Sin embargo, la acción de las ventanas en Firefox es diferente. Las ventanas de Firefox operan con los mismos privilegios de la última ventana abierta. Por ejemplo, si una ventana de Firefox se abre con la sesión de un usuario avanzado, y otra ventana se abre con privilegios de administrador, **ambos** usuarios tendrán privilegios de administrador.

Tabla 5-1. Comportamiento de los privilegios de usuario en exploradores admitidos

Explorador	Acción de las fichas	Acción de las ventanas
Microsoft Internet Explorer 6	No aplicable	Nueva sesión
Microsoft Internet Explorer 7	Desde la última sesión abierta	Nueva sesión
Firefox 2	Desde la última sesión abierta	Desde la última sesión abierta

---

Configuración del NIC del iDRAC6

Esta sección supone que el iDRAC6 ya ha sido configurado y se puede tener acceso al mismo en la red. Consulte "Configurar el sistema de red de iDRAC6" para obtener ayuda con la configuración inicial de la red del iDRAC6.

Configuración de los valores de LAN de IPMI y de red

NOTA: Para poder realizar los pasos a continuación, se debe tener privilegio para **Configurar el iDRAC6**.

NOTA: La mayoría de los servidores DHCP requieren un servidor para guardar un testigo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC) debe proporcionar este símbolo durante la negociación de DHCP. El iDRAC6 proporciona la opción de identificador de cliente con un número de interfaz de un byte (0) seguido de una dirección MAC de seis bytes.

1. Haga clic en **Sistema**→ **Acceso Remoto**→ **iDRAC**.
2. Haga clic en la ficha **Red/Seguridad**.

   Aparecerá la pantalla **Configuración de la red**.
3. Configure los valores de LAN de IPMI y de red, según sea necesario. Consulte la tabla 5-2 y la tabla 5-3 para obtener descripciones de la **Configuración de red** y la **Configuración de LAN de IPMI**.
4. Haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-4.

Tabla 5-2. Configuración de red

Valor	Descripción
Activar NIC	Cuando se selecciona, indica que el NIC está activado y habilita los controles restantes en este grupo. Cuando un NIC está desactivado, toda la comunicación con el iDRAC6 a través de la red está bloqueada.

	El valor predeterminado es **apagado**.
MAC Address	Muestra la dirección de control de acceso al medio (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red. La dirección MAC no se puede cambiar.
Usar DHCP (Para la dirección IP de la tarjeta de interfaz de red)	Pide al iDRAC6 que obtenga una dirección IP para el NIC del servidor de Protocolo de configuración dinámica de host (DHCP). Asimismo, desactiva los controles **Dirección IP estática**, **Máscara de subred estática** y **Puerta de enlace estática**. El valor predeterminado es **apagado**.
Dirección IP estática	Permite ingresar o editar una dirección IP estática para el NIC del iDRAC6. Para cambiar este valor, deseleccione la casilla de marcación **Usar DHCP (para dirección IP del NIC)**.
Máscara de subred estática	Permite ingresar o editar una máscara de subred para el NIC del iDRAC6. Para cambiar este valor, deseleccione primero la casilla de marcación **Usar DHCP (para la dirección IP del NIC)**.
Puerta de enlace estática	Permite ingresar o editar una puerta de enlace estática para el NIC del iDRAC6. Para cambiar este valor, deseleccione primero la casilla de marcación **Usar DHCP (para la dirección IP del NIC)**.
Usar DHCP para obtener direcciones de servidor DNS	Habilite el DHCP para obtener direcciones del servidor DNS por medio de la selección de la casilla **Use el DHCP para obtener direcciones de servidor DNS**. Cuando no se usa DHCP para obtener las direcciones del servidor DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**. El valor predeterminado es **apagado**. **NOTA:** Cuando la casilla **Use el DHCP para obtener direcciones de servidor DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido estático** y **Servidor DNS alternativo estático**.
Servidor DNS preferido estático	Permite al usuario ingresar o editar una dirección IP estática para el servidor DNS preferido. Para cambiar este valor, deseleccione primero la casilla de marcación **Usar DHCP para obtener direcciones de servidor DNS**.
Servidor DNS alternativo estático	Utiliza la dirección IP del servidor DNS secundario cuando la opción **Usar DHCP para obtener direcciones de servidor DNS no está seleccionada**. Introduzca una dirección IP 0.0.0.0 si no hay ningún servidor DNS alternativo.
Registrar el iDRAC en DNS	Registra el nombre del iDRAC6 en el servidor DNS. El valor predeterminado es **Desactivado**.
Nombre DNS del iDRAC	Muestra el nombre del iDRAC6 únicamente cuando la opción **Registrar el iDRAC en DNS** está seleccionada. El nombre predeterminado es idrac-*etiqueta_de_servicio*, donde *etiqueta_de_servicio* es el número de la etiqueta de servicio del servidor Dell. Por ejemplo: idrac-00002.
Usar DHCP para el nombre del dominio de DNS	Utiliza el nombre de dominio DNS predeterminado. Cuando la casilla no está seleccionada y la opción **Registrar el iDRAC en DNS** está seleccionada, usted puede modificar el nombre de dominio DNS en el campo **Nombre de dominio DNS**. El valor predeterminado es **Desactivado**. **NOTA:** Para seleccionar la casilla **Usar DHCP para el nombre del dominio DNS**, seleccione también la casilla **Usar DHCP (para la dirección IP de NIC)**.
Nombre del dominio DNS	El **nombre de dominio DNS** predeterminado está en blanco. Cuando la casilla **Usar DHCP para el nombre del dominio DNS** está seleccionada, esta opción aparece en gris y el campo no se puede modificar.

Tabla 5-3. Configuración de la LAN IPMI

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

Tabla 5-4. Botones de configuración de la red

Botón	Descripción
Configuración avanzada	Abre la pantalla **Seguridad de la red**, lo que permite al usuario ingresar atributos de rango de IP y bloqueo de IP.
Imprimir	Imprime los valores de la **Configuración de red** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **Configuración de red**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la pantalla de configuración de la red. **NOTA:** Si se hacen cambios en la configuración de la dirección IP del NIC se cerrarán todas las sesiones de usuario y los usuarios tendrán que volver a conectarse a la interfaz Web del iDRAC6 con la configuración actualizada de la dirección IP. Todos los demás cambios requerirán que se restablezca la tarjeta de interfaz de red, lo que provocará una breve pérdida de conectividad.

Configuración de la filtración de IP y el bloqueo de IP

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

1. Haga clic en **Sistema**→ **Acceso Remoto**→ **iDRAC.**
2. Haga clic en la ficha **Red/Seguridad**.

   Aparecerá la pantalla **Configuración de la red**.
3. Haga clic en **Configuración avanzada**.

   Aparecerá la pantalla **Seguridad de la red**.
4. Configure los valores de filtro y bloqueo de IP, según sea necesario. Consulte la tabla 5-5 para obtener descripciones de los valores de **filtro y bloqueo de IP**.
5. Haga clic en **Aplicar**.
6. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-6.

Tabla 5-5. Configuración de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de revisión del rango de IP, que define un rango de direcciones IP que pueden acceder al iDRAC6. El valor predeterminado es **apagado**.
Dirección del rango de IP	Determina la dirección de subred de IP aceptable. El valor predeterminado es **192.168.1.0**.
Máscara de subred del rango de IP	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en formato de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior. El valor predeterminado es **255.255.255.0**.
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, lo que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo predefinido. El valor predeterminado es **apagado**.
Número de intentos fallidos para bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección. El valor predeterminado es **10**.
Ventana de intentos fallidos para bloqueo de IP	Determina el periodo en segundos dentro del que debe presentarse el número de intentos fallidos para activar el tiempo de penalización de bloqueo de IP. El valor predeterminado es **3600**.
Tiempo de penalización de bloqueo de IP	El período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas. El valor predeterminado es **3600.**

Tabla 5-6. Botones de seguridad de la red

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

Configuración de los sucesos de plataforma

La configuración de sucesos de plataforma ofrece un mecanismo para configurar el iDRAC6 a fin de realizar las acciones seleccionadas ante ciertos mensajes de sucesos. Las acciones incluyen reiniciar el sistema, sin acción, realizar ciclo de encendido del sistema, apagar el sistema y generar una alerta (captura de sucesos de plataforma [PET] y/o correo electrónico).

Los sucesos de plataforma que se pueden filtrar se muestran en la tabla 5-7.

Tabla 5-7. Sucesos de plataforma que se pueden filtrar

Índice	Suceso de plataforma
1	Declaración de advertencia de la batería
2	Declaración crítica de la batería
3	Declaración crítica de voltaje discreto
4	Declaración de advertencia de temperatura
5	Declaración crítica de temperatura
6	Redundancia degradada
7	Redundancia perdida

8	Declaración de advertencia del procesador
9	Declaración crítica del procesador
10	Declaración de ausencia del procesador
11	Declaración crítica de registro de sucesos
12	Declaración crítica de vigilancia

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

Si el mismo filtro de sucesos de plataforma también está configurado para realizar una acción (por ejemplo, reiniciar el sistema), la acción se ejecutará.

Configuración de los filtros de sucesos de plataforma (PEF)

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

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Haga clic en **Sistema** y luego en la ficha **Administración de alertas**.

   Aparecerá la pantalla **Sucesos de plataforma**.
3. Seleccione la casilla **Generar alerta** al lado de cada suceso para el cual desea que se genere una alerta.

   NOTA: Puede activar o desactivar la generación de alertas para todos los sucesos al seleccionar o deseleccionar la casilla junto al encabezado de la columna **Generar alerta**.
4. Seleccione en el botón de radio debajo de la acción que desea activar para cada suceso. Sólo se puede seleccionar una acción para cada suceso.
5. Haga clic en **Aplicar**.

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

Configuración de capturas de suceso de plataforma (PET)

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

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de los filtros de sucesos de plataforma (PEF)".
3. Haga clic en **Sistema** y luego en la ficha **Administración de alertas**.

   Aparecerá la pantalla **Sucesos de plataforma**.
4. Haga clic en **Configuración de captura**.

   Aparecerá la pantalla **Destinos de alertas de sucesos de plataforma**.
5. Configure la dirección IP de destino de la PET:
   a. Seleccione la casilla **Activar** junto al **Número de destino** que desea activar.
   b. Introduzca una dirección IP en el cuadro **Dirección IP de destino**.

   NOTA: La cadena de la comunidad de destino debe ser la misma que la cadena de la comunidad de iDRAC6.

   c. Haga clic en **Aplicar**.

   NOTA: Para tener éxito en el envío de una captura, configure el valor de la **Cadena de comunidad** en la pantalla **Configuración de la red**. El valor de la **Cadena de comunidad** indica la cadena de comunidad que se va a usar en una captura de alertas de Protocolo simple de administración de red (SNMP) enviada desde el iDRAC6. Las capturas de alertas SNMP son transmitidas por el iDRAC6 cuando ocurre un suceso de plataforma. El valor predeterminado de la **Cadena de comunidad** es **Public**.

   d. Haga clic en **Enviar** para probar la alerta configurada.
   e. Para agregar una dirección de IP de destino adicional, repita del paso a al paso d. Puede especificar hasta cuatro direcciones de IP de destino.

Configuración de alertas por correo electrónico

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Asegúrese de que siguió los procedimientos descritos en "Configuración de los filtros de sucesos de plataforma (PEF)".
3. Haga clic en **Sistema** y luego en la ficha **Administración de alertas**.

   Aparecerá la pantalla **Sucesos de plataforma**.
4. Haga clic en **Configuración de alertas de correo electrónico**.

   Aparecerá la pantalla **Configuración de alertas de correo electrónico**.
5. Configure el destino de la alerta por correo electrónico.
   a. Seleccione la casilla **Activada** para la primera alerta de correo electrónico sin definir.
   b. Escriba una dirección de correo electrónico válida en el campo **Dirección de correo electrónico de destino**.
   c. Haga clic en **Aplicar**.

   NOTA: Para enviar correctamente un correo electrónico de prueba, la **Dirección del servidor SMTP** debe estar configurada en la sección **Configuración de la dirección del servidor (correo electrónico) SMTP** de la pantalla **Configuración de alertas por correo electrónico**. La dirección IP del **Servidor SMTP** se comunica con el iDRAC6 para enviar alertas por correo electrónico cuando ocurre un suceso de plataforma.

   d. Haga clic en **Enviar** para probar la alerta por correo electrónico configurada (si lo desea).
   e. Para agregar un destino de alertas por correo electrónico adicional, repita del paso a al paso d. Puede especificar hasta cuatro destinos de alertas por correo electrónico.

Configuración de IPMI en la LAN

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Configure la IPMI en la LAN:
   a. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**, luego haga clic en la ficha **Red/Seguridad**.

      Aparecerá la pantalla **Configuración de la red**.
   b. Haga clic en **Configuración de la LAN IPMI**.
   c. Seleccione la casilla **Activar IPMI en la LAN**.
   d. Actualice los privilegios del canal de LAN de IPMI, si es necesario:

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

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

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

   NOTA: La IPMI de iDRAC6 es compatible con el protocolo RMCP+.

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

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

   f. Haga clic en **Aplicar**.
3. Configure la comunicación en serie en la LAN (SOL) de IPMI.
   a. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**, luego haga clic en la ficha **Red/Seguridad**.

      Aparecerá la pantalla **Configuración de la red**.
   b. Abra la pantalla **Comunicación en serie en la LAN**.
   c. Seleccione la casilla **Activar comunicación en serie en la LAN**.
   d. Si es necesario, actualice la velocidad en baudios de SOL de IPMI seleccionando un valor en el menú desplegable Velocidad en baudios.

NOTA: Para redirigir la consola serie en la LAN, asegúrese que la velocidad en baudios de SOL sea idéntica a la velocidad en baudios del servidor administrado.

e. Haga clic en **Aplicar**.

Cómo agregar y configurar usuarios de iDRAC6

Para administrar el sistema con el iDRAC6 y mantener la seguridad del sistema, cree usuarios únicos con permisos administrativos específicos (o con *autoridad basada en funciones*).

Para agregar y configurar los usuarios de iDRAC6, realice los pasos siguientes:

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

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

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

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

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

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

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

   La tabla 5-8 describe los valores **Generales** de configuración de un nombre de usuario y contraseña del iDRAC6.

   La tabla 5-9 describe los **Privilegios de la LAN de IPMI** para configurar los privilegios de LAN del usuario.

   La tabla 5-10 describe los permisos del **Grupo de usuarios** para la configuración de los **Privilegios de LAN de IPMI** y de los **Privilegios de usuario del iDRAC**.

   La tabla 5-11 describe los permisos de **Grupo de iDRAC**. Si agrega un **Privilegio de usuario de iDRAC** al grupo de **Administrador**, **Usuario avanzado** o **Usuario invitado**, el **Grupo de iDRAC** cambiará a grupo **Personalizado**.

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

6. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-12.

Tabla 5-8. Propiedades generales

Propiedad	Descripción
Identificación de usuario	Contiene uno de los 16 números preconfigurados de identificación de usuario. Este campo no se puede editar.
Activar el usuario	Cuando está seleccionado, indica que el acceso del usuario al iDRAC6 está activado. Cuando no está seleccionado, el acceso de usuario está desactivado.
Nombre de usuario	Especifica un nombre de usuario de iDRAC6 de hasta 16 caracteres. Cada usuario debe tener un nombre de usuario único. **NOTA:** Los nombres de usuario de iDRAC6 no pueden incluir los caracteres de **/** (diagonal) ni **.** (punto). **NOTA:** Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el siguiente inicio de sesión del usuario.
Cambiar contraseña	Activa los campos **Nueva contraseña** y **Confirmar nueva contraseña**. Cuando está deseleccionada, la **Contraseña** del usuario no se puede cambiar.
Contraseña nueva	Activa la edición de la contraseña del usuario del iDRAC6. Introduzca una **Contraseña** de hasta 20 caracteres. Los caracteres no se mostrarán.
Confirmar nueva contraseña	Vuelva a escribir la contraseña del usuario del iDRAC6 para confirmarla.

Tabla 5-9. Privilegios del usuario en la LAN de IPMI

Propiedad	Descripción
Privilegio máximo permitido de usuario de LAN	Especifica el privilegio máximo del usuario en el canal de LAN de IPMI como uno de los siguientes grupos de usuario: **Ninguno**, **Administrador**, **Operador** o **Usuario**.

Activar comunicación en serie en la LAN.	Permite al usuario usar la comunicación en serie en la LAN de IPMI. Cuando se selecciona, este privilegio se activa.

Tabla 5-10. Privilegios del usuario del iDRAC6

Propiedad	Descripción
Grupo de iDRAC	Especifica el privilegio máximo del usuario de iDRAC6 como uno de los siguientes: **Administrador**, **Usuario avanzado**, **Usuario invitado**, **Personalizado** o **Ninguno**. Consulte la tabla 5-11 para ver los permisos del **Grupo de iDRAC6**.
Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC6.
Configurar iDRAC	Permite al usuario configurar el iDRAC6.
Configurar usuarios	Activa la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros de iDRAC6.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a redirección de consola	Activa la capacidad del usuario de ejecutar redirección de consola.
Acceder a los medios virtuales	Activa la capacidad del usuario de ejecutar y usar los medios virtuales.
Probar alertas	Activa la capacidad del usuario de enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Activa la capacidad del usuario de ejecutar comandos de diagnóstico.

Tabla 5-11. Permisos de grupo del iDRAC6

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

Tabla 5-12. Botones de configuración de usuarios

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

Cómo asegurar las comunicaciones de iDRAC6 por medio de certificados SSL y digitales

Esta sección ofrece información sobre las siguientes funciones de seguridad de datos que vienen incorporadas en el iDRAC6:

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

Capa de conexión segura (SSL)

El iDRAC6 incluye un servidor Web que está configurado para usar el protocolo de seguridad SSL (el estándar de la industria) para transferir datos cifrados a

través de una red. Como está cimentado en la tecnología de cifrado de claves privada y pública, la SSL es una tecnología ampliamente aceptada para proporcionar comunicación cifrada y autentificada entre clientes y servidores a fin de prevenir el espionaje en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

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

El proceso de cifrado proporciona un alto nivel de protección de datos. El iDRAC6 emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está normalmente disponible para los exploradores de Internet en Norteamérica.

De manera predeterminada, el servidor Web de iDRAC6 tiene un certificado digital SSL autofirmado (identificación del servidor) de Dell. Para garantizar una alta seguridad en la Internet, sustituya el certificado de SSL del servidor web con un certificado firmado por una autoridad reconocida de certificados. Para iniciar el proceso de obtención de un certificado firmado, se puede usar la interfaz Web del iDRAC6 para generar una solicitud de firma de certificado (CSR) con la información de la empresa. Usted podrá enviar entonces la CSR generada a una autoridad de certificados como VeriSign o Thawte.

Solicitud de firma de certificado (CSR)

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

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

Después de que la autoridad de certificados apruebe la CSR y envíe el certificado, cargue el certificado en el firmware del iDRAC6. La información de la CSR almacenada en el firmware del iDRAC6 debe coincidir con la información contenida en el certificado.

Acceso al menú principal de SSL

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

Use la pantalla **Menú principal de SSL** para generar una CSR para enviarla a una autoridad de certificados. La información de la CSR se almacena en el firmware del iDRAC6.

La tabla 5-13 describe las opciones disponibles al momento de generar una CSR.

La tabla 5-14 describe los botones disponibles en la pantalla **Menú principal de SSL**.

Tabla 5-13. Opciones del menú principal de SSL

Campo	Descripción
Generar una nueva solicitud de firma de certificado (CSR)	Seleccione la opción y haga clic en **Siguiente** para abrir la pantalla **Generar solicitud de firma de certificado (CSR)**. **NOTA:** Cada nueva CSR sobrescribe la CSR anterior en el firmware. Para que la CA acepte la CSR, la CSR que está en el firmware debe coincidir con el certificado que la CA devuelve.
Cargar certificado de servidor	Seleccione la opción y haga clic en **Siguiente** para abrir la pantalla **Carga del certificado** y cargar el certificado que recibió de la autoridad de certificados. **NOTA:** El iDRAC6 sólo acepta certificados codificados con X509, base 64. No acepta certificados codificados DER.
Ver el certificado de servidor	Seleccione la opción y haga clic en **Siguiente** para abrir la pantalla **Ver certificado del servidor** y acceder a un certificado de servidor existente.

Tabla 5-14. Botones del menú principal de SSL

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

Generación de una nueva solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribirá los datos de la CSR anterior que esté guardada en el firmware. La CSR en el firmware debe coincidir con el certificado que recibió de la autoridad de certificados. De lo contrario, el iDRAC6 no aceptará el certificado.

1. En la pantalla **Menú principal de SSL**, seleccione **Generar una nueva solicitud de firma de certificado (CSR)** y haga clic en **Siguiente**.
2. En la pantalla **Generar solicitud de firma de certificado (CSR)**, introduzca un valor para cada atributo de la CSR.

   La tabla 5-15 describe las opciones de la pantalla **Generar solicitud de firma de certificado (CSR)**.
3. Haga clic en **Generar** para crear la CSR.
4. Haga clic en **Descargar** para guardar el archivo de la CSR en el equipo local.
5. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-16.

Tabla 5-15. Opciones Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre del dominio del servidor web, por ejemplo, **www.empresaxyz.com**). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Unidad organizacional	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Tecnología informática). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	La ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Monterrey). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo u otro carácter.
Nombre del estado:	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Nuevo León). Sólo son válidos los caracteres alfanuméricos y los espacios. No utilice abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Escriba la dirección de correo electrónico de la empresa o cualquier dirección de correo electrónico asociada con la CSR. Este campo es opcional.

Tabla 5-16. Botones para generar una solicitud de firma de certificado (CSR)

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

Carga de un certificado de servidor

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

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

   NOTA: El valor **Ruta de acceso del archivo** muestra la ruta de acceso del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.
3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-17.

Tabla 5-17. Botones de carga de certificados

Botón	Descripción

Imprimir	Imprime los valores que aparecen en la pantalla **Carga del certificado**.
Actualizar	Vuelve a cargar la pantalla **Carga del certificado**.
Aplicar	Aplica el certificado al firmware del iDRAC6
Volver al menú principal de SSL	Regresa al usuario a la pantalla **Menú principal de SSL**.

Cómo ver un certificado de servidor

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

   La tabla 5-18 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-19.

Tabla 5-18. Información de certificados

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

Tabla 5-19. Botones de visualización de certificados del servidor

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

Configuración y administración de certificados de Active Directory

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

NOTA: Para obtener más información acerca de la configuración de Active Directory y sobre cómo configurar Active Directory con el esquema estándar o un esquema ampliado, consulte "Uso de iDRAC6 con Microsoft Active Directory".

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

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

2. Haga clic en **Active Directory** para abrir la pantalla **Menú principal de Active Directory**.

   La tabla 5-20 muestra una lista de las opciones del **Menú principal de Active Directory**.

3. Para continuar, haga clic en el botón correspondiente. Consulte la tabla 5- 20.

   Tabla 5-20. Opciones del menú principal de Active Directory

Campo	Descripción
Configurar Active Directory	Configura los valores **Nombre de dominio raíz**, **Tiempo de espera de autentificación de Active Directory**, **Selección del esquema de Active Directory**, **Nombre del iDRAC**, **Nombre de dominio del iDRAC**, **Grupos de funciones**, **Nombre de grupo** y **Dominio del grupo** de Active Directory.
Cargar un certificado de CA de Active Directory	Carga un certificado de Active Directory en el iDRAC6.
Ver un certificado de CA de Active Directory	Muestra el certificado de Active Directory que ha sido cargado en el iDRAC6.

Tabla 5-21. Botones del menú principal de Active Directory

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

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

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

   La tabla 5-22 describe los valores de la **Configuración y administración de Active Directory**.
3. Haga clic en **Aplicar** para guardar la configuración.
4. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-23.
5. Para configurar los grupos de funciones para el esquema estándar de Active Directory, haga clic en el grupo de funciones individual (1 a 5). Consulte los apartados la tabla 5-24 y la tabla 5-25.

   NOTA: Para guardar los valores de la pantalla **Configuración de Active Directory**, haga clic en **Aplicar** antes de proceder con la página **Grupo de funciones personalizado**.

Tabla 5-22. Valores de configuración de Active Directory

Valor	Descripción
Activar Active Directory	Cuando está seleccionado, activa Active Directory. El valor predeterminado es **desactivado**.
Nombre del dominio RAÍZ	El nombre de dominio RAÍZ de Active Directory. De manera predeterminada está en blanco. El nombre debe ser un nombre de dominio válido que consista de *x.y*, donde *x* es una cadena de 1 a 254 caracteres ASCII sin espacios en blanco entre ellos y *y* es un tipo de dominio válido como com, edu, gov, int, mil, red u org. De manera predeterminada está en blanco.
Tiempo de espera	El tiempo en segundos para completar consultas de Active Directory. El valor mínimo es igual o mayor que 15 segundos. El valor predeterminado es **120**.
Usar el esquema estándar	Usa el esquema estándar con Active Directory.
Usar el esquema ampliado	Usa el esquema ampliado con Active Directory.
Nombre del iDRAC	El nombre que identifica de manera exclusiva el iDRAC6 en Active Directory. De manera predeterminada está en blanco. El nombre debe ser una cadena de 1 a 254 caracteres ASCII, sin espacios entre ellos.
Nombre del dominio de iDRAC	El nombre DNS del dominio donde reside el objeto iDRAC6 de Active Directory. De manera predeterminada está en blanco. El nombre debe ser un nombre de dominio válido que consista de *x.y*, donde *x* es una cadena de 1 a 254 caracteres ASCII sin espacios en blanco entre ellos y *y* es un tipo de dominio válido como com, edu, gov, int, mil, red u org.
Grupos de funciones	La lista de grupos de funciones relacionados con el iDRAC6. Para cambiar la configuración de un grupo de función, haga clic en el número del grupo de funciones, en la lista de grupos de funciones.
Nombre del grupo	El nombre que identifica el grupo de funciones en Active Directory relacionado con el iDRAC6. De manera predeterminada está en blanco.
Dominio de grupo	El tipo de dominio en donde reside el grupo de funciones.

Tabla 5-23. Botones de configuración de Active Directory

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración de Active Directory** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **Configuración de Active Directory**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la pantalla **Configuración de Active Directory**.
Volver al menú principal de Active Directory	Regresa a la pantalla **Menú principal de Active Directory**.

Tabla 5-24. Privilegios del grupo de funciones

Valor	Descripción
Nivel de privilegio del grupo de funciones	Especifica el privilegio máximo del usuario de iDRAC6 como uno de los siguientes: **Administrador**, **Usuario avanzado**, **Usuario invitado**, **Ninguno** o **Personalizado**. Consulte la tabla 5-25 para ver los permisos del **Grupo de funciones.**
Inicio de sesión en iDRAC	Permite que el grupo inicie sesión en el iDRAC6.
Configurar iDRAC	Da permiso al grupo para configurar el iDRAC6.
Configurar usuarios	Da permiso al grupo para configurar usuarios.
Borrar registros	Da permiso al grupo para borrar registros.
Ejecutar comandos de control del servidor	Da permiso al grupo para ejecutar comandos de control del servidor.
Acceder a redirección de consola	Permite que el grupo tenga acceso a la redirección de consola.
Acceder a los medios virtuales	Permite que el grupo tenga acceso a los medios virtuales.
Probar alertas	Permite al grupo enviar alertas de prueba (mensajes de correo electrónico y capturas de sucesos de plataforma) a un usuario específico.
Ejecutar comandos de diagnóstico	Da permiso al grupo para ejecutar comandos de diagnóstico.

Tabla 5-25. Permisos del grupo de funciones

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

Cómo cargar un certificado de CA de Active Directory

1. En la pantalla **Menú principal de Active Directory**, seleccione **Cargar certificado de CA de Active Directory** y haga clic en **Siguiente**.
2. En la **pantalla Carga de certificado,** escriba la ruta de acceso del certificado en el campo **Ruta de acceso del archivo** o haga clic en **Examinar** para desplazarse al archivo de certificado.

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

Asegúrese de que los certificados SSL del controlador de dominio estén firmados por la misma autoridad de certificados y que el certificado esté disponible en la estación de administración que esté accediendo al iDRAC6.

3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-26.

Tabla 5-26. Botones de carga de certificados

Botón	Descripción
Imprimir	Imprime los valores de **Carga del certificado** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la página **Carga del certificado**.
Aplicar	Aplica el certificado al firmware del iDRAC6
Volver al menú principal de Active Directory	Regresa a la pantalla **Menú principal de Active Directory**.

Cómo ver un certificado de CA de Active Directory

Use la pantalla **Menú principal de Active Directory** para ver un certificado de servidor de CA de iDRAC6.

1. En la pantalla **Menú principal de Active Directory**, seleccione **Ver certificado de CA de Active Directory** y haga clic en **Siguiente**.

La tabla 5-27 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

2. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-28.

Tabla 5-27. Información del certificado de CA de Active Directory

Campo	Descripción
Número de serie	El número de serie del certificado.
Información del titular	Los atributos del certificado introducidos por el titular.
Información del emisor	Los atributos del certificado generados por el emisor.
Válido desde	La fecha de emisión del certificado.
Válido hasta	La fecha de expiración del certificado.

Tabla 5-28. Botones para ver el certificado de CA de Active Directory

Botón	Descripción
Imprimir	Imprime los **valores del certificado de CA de Active Directory que aparecen en la pantalla**.
Actualizar	Vuelve a cargar la **pantalla Certificado de CA de Active Directory**.
Volver al menú principal de Active Directory	Regresa al usuario a la pantalla **Menú principal de Active Directory**.

Activación o desactivación del acceso a la configuración local

NOTA: La configuración predeterminada para el acceso a la configuración local es **Activado**.

Activación del acceso a la configuración local

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**.
2. En **Configuración local**, haga clic para deseleccionar la casilla **Desactivar actualizaciones de Configuración de USUARIO iDRAC local** para activar el acceso.
3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-34.

Desactivación del acceso a la configuración local

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**.
2. En **Configuración local**, haga clic para deseleccionar la casilla **Desactivar actualizaciones de Configuración de USUARIO iDRAC local** para activar el acceso.
3. Haga clic en **Aplicar**.
4. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-34.

Configuración de los servicios de iDRAC6

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC**.

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

NOTA: Existe un problema conocido con el cliente Telnet suministrado con Microsoft Windows y la comunicación con una BMU. Use otro cliente Telnet como HyperTerminal o PuTTY.

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

2. Haga clic en **Servicios** para abrir la pantalla de configuración **Servicios**.

3. Configure los servicios siguientes según sea necesario:
   - Servidor web: consulte la tabla 5-29 para ver la configuración del servidor web
   - SSH: consulte la tabla 5-30 para ver la configuración de SSH
   - Telnet: consulte la tabla 5-31 para ver la configuración de Telnet
   - Agente SNMP: consulte la tabla 5-32 para obtener información sobre la configuración del agente SNMP
   - Agente de recuperación automatizada del sistema: consulte la tabla 5-33 para ver la configuración del agente de recuperación automatizada del sistema

4. Haga clic en **Aplicar**.

5. Para continuar, haga clic en el botón correspondiente. Vea la tabla 5-34.

Tabla 5-29. Configuración del servidor Web

Valor	Descripción
Activado	Activa o desactiva el servidor Web del iDRAC6. Cuando está seleccionada, indica que el servidor Web está activado. El valor predeterminado es **activado**.
N° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Este campo no se puede editar. Pueden existir cuatro sesiones simultáneas.
Sesiones actuales	El número de sesiones actuales en el sistema, menor o igual al **N.° máx. de sesiones**. Este campo no se puede editar.
Tiempo de espera	El tiempo, en segundos, permitido para que la conexión permanezca inactiva. La sesión se cierra cuando se alcanza el tiempo de espera. Los cambios en el valor de tiempo de espera surtirán efecto inmediatamente y restablecerán el servidor Web. El rango del tiempo de espera es de 60 a 10800 segundos. El valor predeterminado es de **1800** segundos.
Número de puerto de HTTP	El puerto en el que el iDRAC6 espera una conexión de explorador. El valor predeterminado es **80**.
Número de puerto de HTTPS	El puerto en el que el iDRAC6 espera una conexión de explorador segura. El valor predeterminado es **443**.

Tabla 5-30. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Cuando está seleccionada, la casilla indica que SSH está activado.
N° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Sólo se admite una sesión.
Sesiones activas	El número de sesiones actuales en el sistema.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango del tiempo de espera es de 60 a 10800 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **1800.**
Número de puerto	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es **22**.

Tabla 5-31. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando se selecciona, Telnet está activado. El valor predeterminado es **desactivado**.
N° máx. de sesiones	El número máximo de sesiones simultáneas que se permite para este sistema. Sólo se admite una sesión.
Sesiones activas	El número de sesiones actuales en el sistema.
Tiempo de espera	El tiempo de espera en inactividad del telnet, en segundos. El rango del tiempo de espera es de 60 a 10800 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **1800.**
Número de puerto	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es **23**.

Tabla 5-32. Agente SNMP

Valor	Descripción
Activado	Activa o desactiva las alertas de correo electrónico.
Nombre de comunidad SNMP	El nombre de la comunidad que contiene la dirección IP del destino de alertas SNMP. El nombre de comunidad puede tener hasta 31 caracteres sin espacios. Valor predeterminado=público.

Tabla 5-33. Configuración del agente de recuperación automatizada del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automatizada del sistema.

Tabla 5-34. Botones de servicios

Botón	Descripción
Imprimir	Imprime la pantalla **Servicios**.
Actualizar	Actualiza la pantalla **Servicios**.
Aplicar cambios	Aplica los valores de la pantalla **Servicios**.

Actualización del firmware de iDRAC6

NOTA: Si el firmware del iDRAC6 se daña, como puede suceder cuando el progreso de la actualización del firmware del iDRAC6 se interrumpe antes de terminar, puede recuperar el iDRAC6 por medio del CMC. Consulte su *Guía del usuario del firmware del CMC* para obtener instrucciones.

NOTA: De manera predeterminada, la actualización del firmware retendrá la configuración actual del iDRAC6. Durante el proceso de actualización, tiene la opción de restablecer la configuración predeterminada de fábrica del iDRAC6. Si usted establece la configuración predeterminada de fábrica, el acceso a la red externa se desactivará cuando la actualización termine. Debe activar y configurar la red por medio de la utilidad de configuración del iDRAC6 o la interfaz Web del CMC.

1. Inicie la interfaz Web del iDRAC6.
2. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**, luego haga clic en la ficha **Actualizar**.

   NOTA: Para actualizar el firmware, el iDRAC6 debe estar en el modo de actualización. Cuando se encuentre en este modo, el iDRAC6 se restablecerá automáticamente, aun cuando usted cancele el proceso de actualización.

3. En la pantalla **Actualización del firmware**, haga clic en **Siguiente** para iniciar el proceso de actualización.
4. En la ventana **Actualización del firmware: Cargar (página 1 de 4)**, haga clic en **Examinar** o escriba la ruta de acceso de la imagen del firmware que descargó.

   Por ejemplo:

   `C:\Updates\V2.0\<image_name>`.

   El nombre predeterminado de la imagen del firmware es **firmimg.imc**.

5. Haga clic en **Siguiente**.
   - El archivo se cargará en el iDRAC6. This may take several minutes to complete.

     O bien:

   - Puede hacer clic en **Cancelar** en este momento si lo que desea es terminar el proceso de actualización de firmware. Al hacer clic en **Cancelar,** el iDRAC6 se restablecerá al modo de operación normal.
6. En la ventana **Actualización del firmware: Validación (página 2 de 4)**, verá los resultados de la validación hecha en el archivo de imagen que cargó.
   - Cuando el archivo de imagen se cargue exitosamente y pase todas las revisiones de verificación, aparecerá un mensaje indicando que la imagen del firmware ha sido verificada.

     O bien:

   - Cuando la imagen no se cargue correctamente o cuando no pase las revisiones de verificación, la actualización del firmware regresará a la ventana **Actualización del firmware: Cargar (página 1 de 4)**. Puede intentar actualizar el iDRAC6 nuevamente o hacer clic en **Cancelar** para restablecer el iDRAC6 al modo de operación normal.

   NOTA: Si deselecciona la casilla **Conservar configuración**, el iDRAC6 restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está desactivada. Usted no podrá iniciar sesión en la interfaz Web del iDRAC6. Deberá reconfigurar los valores de la LAN por medio de la interfaz Web del CMC o iKVM mediante la utilidad de configuración del iDRAC6 durante la POST del BIOS.

7. De manera predeterminada, la casilla **Conservar configuración** está seleccionada para conservar los valores actuales en el iDRAC6 después de una actualización. Si no desea conservar los valores, deseleccione la casilla **Conservar configuración**.
8. Haga clic en **Comenzar la actualización** para iniciar el proceso de actualización. No interrumpa el proceso de actualización.

9. En la ventana **Actualización del firmware: Actualización (página 3 de 4)**, verá el estado de la actualización. El progreso de la operación de actualización de firmware, expresado en porcentaje, aparecerá en la columna **Progreso**.

10. Una vez que la actualización del firmware concluya, aparecerá la ventana **Actualización del firmware: Resultados de la actualización (página 4 de 4)** y el iDRAC6 se restablecerá automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 usando una ventana nueva de explorador.

Actualización del firmware del iDRAC6 por medio del CMC

Normalmente, el firmware del iDRAC6 se actualiza por medio de las utilidades de iDRAC6, por ejemplo, la interfaz Web del iDRAC6 o los paquetes de actualización específicos del sistema operativo que descargó de **support.dell.com**.

Puede usar la interfaz Web del CMC o RACADM del CMC para actualizar el firmware de iDRAC6. Esta función está disponible cuando el firmware del iDRAC6 está en modo Normal y cuando está dañado. Consulte "Actualización del firmware del iDRAC6 por medio del CMC"].

NOTA: Consulte la *Guía del usuario del firmware del Chassis Management Controller* para obtener instrucciones sobre cómo usar la interfaz Web del CMC.

Para actualizar el firmware del iDRAC6, realice los pasos siguientes:

1. Descargue el firmware del iDRAC6 más reciente en el equipo de administración de la dirección **support.dell.com**.

2. Inicie sesión en la interfaz basada en web de la CMC.

3. Haga clic en **Chassis** (Chasis) en el árbol del sistema.

4. Haga clic en la ficha **Update** (Actualizar). Aparecerá la pantalla **Componentes actualizables**.

5. Haga clic en **servidor-*n***, donde ***n*** es el número del servidor cuyo iDRAC6 desea actualizar.

6. Haga clic en **Examinar,** acceda a la imagen del firmware del iDRAC6 que descargó y haga clic en **Abrir**.

7. Haga clic en **Iniciar actualización del firmware**.

Después de que el archivo de la imagen del firmware ha sido cargado en CMC, el iDRAC6 se actualizará a sí mismo con la imagen.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de iDRAC6 con Microsoft Active Directory

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Un servicio de directorio se usa para mantener una base de datos común de toda la información necesaria para controlar a usuarios, equipos, impresoras, etc., en una red. Si la empresa usa el software de servicio Microsoft® Active Directory®, puede configurarlo de manera que tenga acceso al iDRAC6, lo que le permite agregar privilegios de usuario de iDRAC6 a los usuarios existentes y controlar estos privilegios en el software Active Directory.

NOTA: El uso de Active Directory para reconocer usuarios del iDRAC6 se admite en los sistemas operativos Microsoft Windows 2000, Windows Server 2003 y Windows Server 2008.

La tabla 6-1 muestra los nueve privilegios de usuario de Active Directory del iDRAC6.

Tabla 6-1. Privilegios de usuario del iDRAC6

Privilegio	Descripción
Inicio de sesión en iDRAC	Permite al usuario iniciar sesión en el iDRAC6.
Configurar iDRAC	Permite al usuario configurar iDRAC6.
Configurar usuarios	Permite al usuario otorgar acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros de iDRAC6.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a redirección de consola	Permite al usuario ejecutar la redirección de consola.
Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.
Probar alertas	Permite al usuario enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Requisitos previos para activar la autentificación de Active Directory para iDRAC6

Para usar la función de autentificación de Active Directory del iDRAC6, debe haber implementado una infraestructura de Active Directory. Consulte el sitio web de Microsoft para obtener información sobre cómo configurar una infraestructura de Active Directory si aún no tiene una.

El iDRAC6 utiliza el mecanismo estándar de infraestructura de clave pública (PKI) para autentificar de manera segura en Active Directory, por lo tanto, necesitará también una PKI integrada en la infraestructura de Active Directory.

Consulte el sitio Web de Microsoft para obtener más información sobre la configuración de PKI.

Para autentificar correctamente todos los controladores de dominio, también necesitará activar la Capa de conexión segura (SSL) en todos los controladores de dominio a los que se conecte el iDRAC6. Consulte "Activación de SSL en un controlador de dominio" para obtener información más específica.

Mecanismos de autenticación compatibles de Active Directory

Puede utilizar Active Directory para definir el acceso de los usuarios en el iDRAC6 mediante dos métodos: mediante la solución de *esquema ampliado*, que Dell ha personalizado para agregar objetos de Active Directory definidos por Dell. O puede usar la solución de *esquema estándar*, que utiliza únicamente objetos de grupo de Active Directory. Consulte las secciones siguientes para obtener más información sobre estas soluciones.

Cuando se usa Active Directory para configurar el acceso al iDRAC6, se debe elegir la solución de esquema ampliado o de esquema estándar.

Las ventajas de usar la solución de esquema ampliado son:

- Todos los objetos de control de acceso se mantienen en Active Directory.
- Se brinda máxima flexibilidad para configurar el acceso de los usuarios en diferentes tarjetas del iDRAC6 con distintos niveles de privilegios.

La ventaja de utilizar la solución de esquema estándar radica en que no se requiere una ampliación del esquema, ya que la configuración predeterminada del esquema de Active Directory que brinda Microsoft proporciona todas las clases de objetos necesarias.

Generalidades del esquema ampliado de Active Directory

Para utilizar la solución de esquema ampliado, es necesaria una ampliación de esquema de Active Directory según se describe en la siguiente sección.

Extensión del esquema de Active Directory

Importante: la ampliación del esquema para este producto es distinta de la de generaciones anteriores de productos de Dell Remote Management. Deberá ampliar el nuevo esquema e instalar el nuevo complemento **Microsoft Management Console (MMC) de usuarios y equipos de Active Directory en** su directorio. El esquema anterior no funciona con este producto.

NOTA: La ampliación del nuevo esquema y la instalación de la nueva ampliación en el complemento de usuarios y equipos de Active Directory no afectan las versiones anteriores del producto.

Puede encontrar el complemento MMC de usuarios y equipos de Active Directory y la ampliación de esquema en el DVD *Dell Systems Management Tools and Documentation*. Para obtener más información, consulte "Extensión del esquema de Active Directory" e "Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory". Para obtener más detalles sobre la ampliación del esquema para iDRAC6 y la instalación del complemento MMC de usuarios y equipos de Active Directory, consulte la *Guía del usuario de instalación y seguridad de Dell OpenManage* en **support.dell.com\manuals**.

NOTA: Cuando crea objetos de asociación o de dispositivo del iDRAC6, asegúrese de seleccionar **Dell Remote Management Object Advanced**.

Extensiones de esquemas de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase que se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario incluyen el nombre y el apellido del usuario, el número telefónico, etc. Las empresas pueden ampliar la base de datos de Active Directory al agregar sus propios atributos y clases únicos para solucionar necesidades específicas del entorno. Dell ha ampliado el esquema para incluir los cambios necesarios para admitir la autentificación y autorización de administración remota.

Cada atributo o clase que es se agrega a un esquema existente de Active Directory debe ser definida con una identificación única. Para mantener identificaciones únicas en toda la industria, Microsoft mantiene una base de datos de Identificadores de objeto de Active Directory (OID) de modo que, cuando las compañías agreguen extensiones al esquema, se pueda garantizar que serán únicas y no entrarán en conflicto una con otra. Para ampliar el esquema en Microsoft Active Directory, Dell recibió OID exclusivos, extensiones de nombre exclusivas e identificaciones de atributo vinculadas exclusivamente para las clases y los atributos agregados al servicio de directorio.

- La extensión de Dell es: `dell`
- Dell base OID es: `1.2.840.113556.1.8000.1280`
- El rango del LinkID de RAC es: `12070 a 12079`

Descripción de las extensiones de esquema del iDRAC6

Para proporcionar la mayor flexibilidad en la multitud de entornos de cliente, Dell proporciona un grupo de propiedades que el usuario puede configurar según los resultados deseados. Dell ha ampliado el esquema para incluir propiedades de asociación, dispositivo y privilegio. La propiedad de asociación se usa para vincular a los usuarios o los grupos que tienen un conjunto específico de privilegios para uno o varios dispositivos del iDRAC6. Este modelo proporciona máxima flexibilidad al Administrador con respecto a las diferentes combinaciones de usuarios, privilegios del iDRAC6 y dispositivos del iDRAC6 en la red sin aumentar demasiado la complejidad.

Descripción general de los objetos de Active Directory

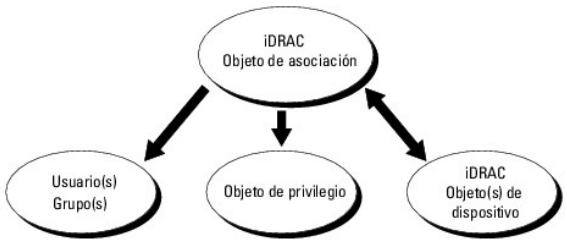
Por cada uno de los dispositivos iDRAC6 físicos de la red que desee integrar con Active Directory para autentificación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo del iDRAC6. Puede crear varios objetos de asociación, y cada objeto de asociación puede vincularse a cuantos usuarios, grupos de usuarios u objetos de dispositivo del iDRAC6 sea necesario. Los usuarios y los grupos de usuarios del iDRAC6 pueden ser miembros de cualquier dominio de la empresa.

Sin embargo, cada objeto de asociación puede vincularse (o puede vincular usuarios, grupos de usuarios u objetos de dispositivo del iDRAC6) sólo a un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en dispositivos iDRAC6 específicos.

El objeto del dispositivo del iDRAC6 es el vínculo al firmware del iDRAC6 para consultar Active Directory para autentificación y autorización. Cuando se agrega el iDRAC6 a la red, el administrador debe configurar el iDRAC6 y su objeto de dispositivo con su nombre de Active Directory para que los usuarios puedan realizar la autentificación y la autorización con Active Directory. Además, el administrador debe agregar iDRAC6 a un objeto de asociación por lo menos para que los usuarios se puedan autentificar.

La figura 6-1 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autenticaciones y autorizaciones.

Figura 6-1. Configuración típica de los objetos de Active Directory



Usted puede crear tantos objetos de asociación como sea necesario. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo del iDRAC6 por cada dispositivo iDRAC6 de la red que desea integrar con Active Directory para autentificación y autorización con iDRAC6.

El objeto de asociación permite toda cantidad de usuarios o grupos, así como de objetos de dispositivo del iDRAC6. 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* de los dispositivos iDRAC6.

La extensión de Dell al complemento MMC de ADUC sólo permite asociar el objeto de privilegio y los objetos del iDRAC6 del mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto iDRAC6 de otro dominio se agregue como miembro del producto del objeto de asociación.

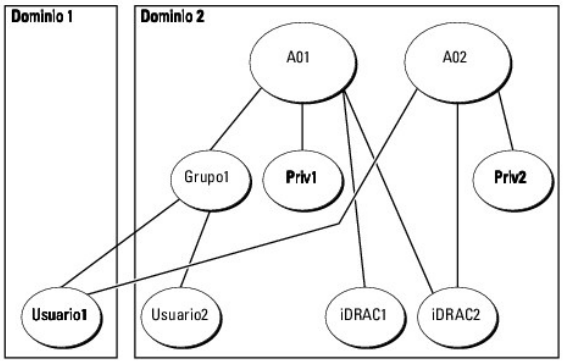
Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio pueden agregarse al objeto de asociación. Las soluciones de esquema ampliado admiten todo tipo de grupos de usuarios o todo grupo anidado de usuarios en varios dominios permitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema ampliado

El mecanismo de autenticación del esquema ampliado admite la acumulación de privilegios provenientes de distintos objetos de privilegio asociados con el mismo usuario entre distintos objetos de asociación. En otras palabras, la autenticación del esquema ampliado acumula privilegios para permitir al usuario el súper conjunto de todos los privilegios asignados que corresponden a los distintos objetos de privilegio asociados al mismo usuario.

La figura 6-2 muestra un ejemplo de la acumulación de privilegios por medio del esquema ampliado.

Figura 6-2. Acumulación de privilegios para un usuario



La figura muestra dos objetos de asociación: OA1 y OA2. El Usuario1 está asociado con el iDRAC2 por medio de ambos objetos de asociación. Por lo tanto, el Usuario1 ha acumulado privilegios que resultan de la combinación del conjunto de privilegios de los objetos Priv1 y Priv2 en iDRAC2.

Por ejemplo, Priv1 tiene los privilegios: Inicio de sesión, Medios virtuales y Borrar registros; y Priv2 tiene los privilegios: Inicio de sesión en iDRAC, Configurar el iDRAC y Probar alertas. Como resultado, el Usuario1 tiene ahora el conjunto de privilegios: Inicio de sesión en iDRAC, Medios virtuales, Borrar registros, Configurar el iDRAC y Probar alertas, que es el conjunto de privilegios combinados de Priv1 y Priv2.

La autentificación del esquema ampliado acumula privilegios para permitir que el usuario tenga el conjunto máximo de privilegios según los privilegios asignados de los distintos objetos de privilegio asociados al mismo usuario.

En esta configuración, el Usuario1 tiene privilegios de Priv1 y Priv2 en iDRAC2. El Usuario1 tiene privilegios de Priv1 en iDRAC1 solamente. El Usuario2 tiene privilegios de Priv1 tanto en iDRAC1 como en iDRAC2. Además, esta ilustración muestra que el Usuario1 puede estar en un dominio diferente y ser miembro de un grupo.

Configuración de Active Directory con esquema ampliado para acceder al iDRAC6

Antes de usar Active Directory para acceder al iDRAC6, debe configurar el software Active Directory y el iDRAC6. Para hacerlo, lleve a cabo los pasos siguientes en el orden indicado:

1. Amplíe el esquema de Active Directory (consulte "Extensión del esquema de Active Directory").
2. Amplíe el complemento de usuarios y equipos de Active Directory (consulte "Instalación de la extensión de Dell para el complemento de usuarios y equipos de Active Directory").

3. Agregue usuarios del iDRAC6 y sus privilegios a Active Directory (consulte "Cómo agregar usuarios y privilegios del iDRAC6 a Active Directory").

4. Active SSL en cada uno de los controladores de dominio (consulte "Activación de SSL en un controlador de dominio").

5. Configure las propiedades de Active Directory del iDRAC6 por medio de la interfaz web del iDRAC6 o RACADM (consulte "Configuración de Active Directory con esquema ampliado con la interfaz basada en web del iDRAC6" o "Configuración de Active Directory con esquema ampliado por medio de RACADM").

La ampliación del esquema de Active Directory agrega una unidad organizacional Dell, clases de esquema y atributos, y los privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de ampliar el esquema, compruebe que tiene privilegios de administrador de esquema en el propietario de la función de operación maestra simple y flexible (FSMO) del esquema en el bosque de dominio.

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

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

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

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

- *Unidad de DVD*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <Unidad *de DVD*>***:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender***

Para usar los archivos LDIF, consulte las instrucciones en el archivo readme (léame) que está en el directorio **LDIF_Files**. Para usar Dell Schema Extender para ampliar el esquema de Active Directory, consulte "Uso del ampliador de esquema de Dell".

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

Uso del ampliador de esquema de Dell

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

1. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.

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

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

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

5. Haga clic en **Finish** (Finalizar).

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

   - Clases (consulte de la tabla 6-2 a la tabla 6-7)
   - Atributos (tabla 6-8)

   Consulte la documentación de Microsoft para obtener información acerca de cómo utilizar el complemento de esquema de Active Directory y MMC.

Tabla 6-2. Definiciones de las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 6-3. Clase dellRacDevice

OID	**1.2.840.113556.1.8000.1280.1.7.1.1**
Descripción	Representa el dispositivo iDRAC6 de Dell. iDRAC6 debe estar configurado como delliDRACDevice en Active Directory. Esta configuración permite que el iDRAC6 envíe consultas de Protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural

SuperClasses	dellProduct
Atributos	**dellSchemaVersion** **dellRacType**

Tabla 6-4. Clase delliDRACAssociationObject

OID	**1.2.840.113556.1.8000.1280.1.7.1.2**
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Grupo
Atributos	**dellProductMembers** **dellPrivilegeMember**

Tabla 6-5. Clase dellRAC4Privileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
Descripción	Define los privilegios (Derechos de autorización) para iDRAC6
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tabla 6-6. Clase dellPrivileges

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	**dellRAC4Privileges**

Tabla 6-7. Clas dellProduct

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

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

Nombre del atributo/Descripción	**OID asignado/Identificador de objeto de sintaxis**	**Con un solo valor**
dellPrivilegeMember Lista de los objetos de dellPrivilege Dell que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

dellProductMembers Lista de los objetos dellRacDevice y DelliDRACDevice que pertenecen a esta función. Este atributo es el vínculo de avance al vínculo de retroceso de dellAssociationMembers. Identificación de vínculo: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE si el usuario tiene derechos de borrado de registro en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de redirección de consola en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.8 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si el usuario tiene derechos de usuario de prueba de alertas en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin TRUE si el usuario tiene derechos de administrador de comandos de depuración en el dispositivov.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Este atributo es el tipo de RAC actual para el objeto delliDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el enlace de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distinguido (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

Cuando se amplía el esquema en Active Directory, también debe ampliarse el complemento de usuarios y equipos de Active Directory para que el administrador pueda administrar los dispositivos iDRAC6, los usuarios y los grupos de usuarios del iDRAC6, y las asociaciones y privilegios del iDRAC6.

Cuando instala el software de administración de sistemas con el DVD **Dell Systems Management Tools and Documentation**, puede ampliar el complemento si selecciona la opción *Complemento de usuarios y equipos de Active Directory* durante el procedimiento de instalación. Consulte la *Guía de instalación rápida del software Dell OpenManage* para obtener más instrucciones sobre la instalación del software de administración de sistemas. Para sistemas operativos de Windows de 64 bits, el programa de instalación del complemento se encuentra en :

<Unidad de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

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

Instalación de Administrator Pack

Debe instalar el paquete de administrador en cada sistema que administre los objetos iDRAC6 de Active Directory. Si no instala el paquete de administrador,

no podrá ver el objeto iDRAC6 de Dell en el contenedor.

Consulte "Cómo abrir el complemento de usuarios y equipos de Active Directory" para obtener más información.

Cómo abrir el complemento de usuarios y equipos de Active Directory

Cómo abrir el complemento de usuarios y equipos de Active Directory:

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

   Si no ha iniciado sesión en el controlador de dominio, el paquete de administrador de Microsoft correspondiente debe estar instalado en el sistema local. Para instalar el paquete de administrador, haga clic en **Inicio→ Ejecutar**, escriba `MMC`, y presione **Entrar**.

   Aparece MMC.

2. En la ventana **Consola 1**, haga clic en **Archivo** (o en **Consola**, en los sistemas que ejecutan Windows 2000).

3. Haga clic en **Agregar o quitar complemento**.

4. Seleccione el **Complemento de usuarios y equipos de Active Directory** y haga clic en **Agregar.**

5. Haga clic en **Cerrar** y haga clic en **Aceptar**.

Cómo agregar usuarios y privilegios del iDRAC6 a Active Directory

El complemento de usuarios y equipos de Active Directory ampliado por Dell permite agregar usuarios y privilegios del iDRAC6 mediante la creación de objetos de asociación y de privilegio del iDRAC6. Para agregar cada tipo de objeto, realice los pasos a continuación:

- Cree un objeto de dispositivo del iDRAC6
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Creación de un objeto del dispositivo del iDRAC6

1. En la ventana **Raíz de la consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.

2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Aparece la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del iDRAC6 que usted va a introducir en el Paso A de "Configuración de Active Directory con esquema ampliado con la interfaz basada en web del iDRAC6".

4. Seleccione Objeto de dispositivo de **iDRAC**.

5. Haga clic en **Aceptar**.

Creación de un objeto de privilegio

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

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.

2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Aparece la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto.

4. Seleccione **Objeto de privilegio**.

5. Haga clic en **Aceptar**.

6. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.

7. Haga clic en la ficha **Privilegios de administración remota** y seleccione los privilegios que desee otorgar al usuario o grupo (consulte la tabla 5-10).

Creación de un objeto de asociación

NOTA: El objeto de asociación del iDRAC6 se deriva de un grupo y su alcance está establecido en Local de dominio.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.

2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Esto abrirá la ventana **Nuevo objeto**.

3. Escriba un nombre para el nuevo objeto.

4. Seleccione **Objeto de asociación**.

5. Seleccione el ámbito para el **objeto de asociación**.

6. Haga clic en **Aceptar**.

Cómo agregar objetos a un objeto de asociación

En la ventana **Propiedades de objeto de asociación**, puede asociar usuarios o grupos de usuarios, objetos de privilegio y dispositivos del iDRAC6 o grupos de dispositivos del iDRAC6.

Puede agregar grupos de usuarios y dispositivos de iDRAC6. 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 del grupo de usuarios o del usuario y haga clic en **Aceptar**.

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 **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentifican en un dispositivo iDRAC6. Sólo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar dispositivos iDRAC6 o grupos de dispositivos iDRAC6

Para agregar dispositivos iDRAC6 o grupos de dispositivos iDRAC6:

1. Seleccione la ficha **Productos** y haga clic en **Agregar.**

2. Escriba el nombre de los dispositivos iDRAC6 o de los grupos de dispositivos iDRAC6 y haga clic en **Aceptar**.

3. En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

Haga clic en la ficha **Productos** para agregar un dispositivo iDRAC6 conectado a la red disponible para los usuarios o grupos de usuarios definidos. Puede agregar varios dispositivos iDRAC6 a un objeto de asociación.

Configuración de Active Directory con esquema ampliado con la interfaz basada en web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz basada en web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**.

   Aparece la pantalla **Información iDRAC**.
4. Haga clic en la ficha **Seguridad de la red** y luego haga clic en **Active Directory**.

   Aparece la pantalla **Configuración y administración de Active Directory**.
5. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

   Aparece la pantalla **Paso 1 de 4 Configuración y administración de Active Directory**.
6. Para validar el certificado SSL de los servidores Active Directory, seleccione la casilla **Activar validación de certificados** en **Configuración de certificados.**

   Si no desea validar el certificado SSL de los servidores Active Directory, no realice ninguna acción; proceda a paso 8.
7. En **Cargar un certificado de CA de Active Directory**, escriba la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado y haga clic en **Cargar.**

   NOTA: Debe escribir la ruta completa de acceso al archivo, que incluye la ruta completa de acceso y el nombre y la extensión completos del archivo.

   La información del certificado para el certificado de CA de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.
8. Haga clic en **Siguiente**.

   Aparece la pantalla **Paso 2 de 4 Configuración y administración de Active Directory**.
9. Seleccione la casilla de marcación **Activar Active Directory.**
10. Haga clic en **Agregar** para ingresar el nombre de dominio de usuario en el campo de texto y luego haga clic en **Aceptar**.
11. Escriba el nombre de dominio de usuario en el indicador y haga clic en **Aceptar**. Tenga en cuenta que este paso es opcional. Si configura una lista de dominios de usuario, la lista estará disponible en la pantalla de inicio de sesión de la interfaz basada en web. Usted puede elegir de la lista y luego sólo debe ingresar el nombre de usuario.
12. En el campo **Tiempo de espera,** ingrese la cantidad de segundos que desea que el iDRAC6 aguarde para las respuestas de Active Directory. El valor predeterminado es 120 segundos.
13. Ingrese la **Dirección de servidor del controlador de dominio.** Puede ingresar hasta tres servidores Active Directory para procesar los inicios de sesión, pero debe configurar al menos un servidor. Para hacerlo, ingrese la dirección IP o el nombre de dominio completo (FQDN). iDRAC6 intenta conectarse a cada servidor configurado hasta establecer una conexión.

    NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo **Sujeto** o **Nombre alternativo de sujeto** del certificado de controlador de dominio si tiene activada la validación de certificado.
14. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 3 de 4 Configuración y administración de Active Directory**.
15. En **Selección del esquema**, seleccione la casilla **Esquema ampliado.**
16. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 4 de 4 Configuración y administración de Active Directory**.
17. En **Configuración de esquema ampliado**, ingrese el nombre del iDRAC6 y el nombre de dominio del iDRAC6 para configurar el objeto de dispositivo del iDRAC6 y su ubicación en Active Directory.
18. Haga clic en **Finalizar** para guardar los cambios y luego en **Finalizado**.

    Aparece la pantalla **Configuración y administración de Active Directory.** A continuación, debe probar los valores de Active Directory que ha configurado.

19. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configuración de prueba.**

    Aparece la pantalla **Configuración de prueba de Active Directory**.

20. Ingrese su nombre de usuario y contraseña del iDRAC6 y luego haga clic en **Iniciar prueba**.

    Aparecen los resultados y el registro de la prueba. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC6 para admitir el inicio de sesión en Active Directory. Vaya a la pantalla **Configuración de red** (haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC** y luego haga clic en la ficha **Red/seguridad**) para configurar los servidores DNS en forma manual o use DHCP para obtener los servidores DNS.

Ha completado la configuración de Active Directory con esquema ampliado.

Configuración de Active Directory con esquema ampliado por medio de RACADM

Use los siguientes comandos para configurar la función de Active Directory del iDRAC6 con esquema ampliado por medio de la herramienta de interfaz de línea de comandos (CLI) de RACADM en lugar de hacerlo mediante la interfaz basada en web.

1. Abra un indicador de comandos y escriba los siguientes comandos de RACADM:

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

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

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

   ```
   racadm config -g cfgActiveDirectory -o cfgADRacDomain <nombre completo del dominio del RAC>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   NOTA: Debe configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. En el esquema ampliado, se trata de las direcciones IP o el FQDN de los controladores de dominio donde se ubica el dispositivo iDRAC6. Los servidores del catálogo global no se utilizan en el modo de esquema ampliado.

   Si desea desactivar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

   ```
   racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
   ```

   En este caso, no tiene que cargar un certificado de CA.

   Si desea aplicar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

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

   En este caso, deberá cargar un certificado de CA con el siguiente comando de RACADM:

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

   El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "Cómo importar el certificado SSL de firmware del iDRAC6".

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

2. Si DHCP está activado en el iDRAC6 y desea usar el DNS proporcionado por el servidor DHCP, escriba el siguiente comando de RACADM:

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

3. Si DHCP está desactivado en el iDRAC6 o si desea introducir manualmente la dirección IP del DNS, escriba los siguientes comandos de RACADM:

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

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

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

4. Si desea configurar una lista de dominios de usuario para ingresar el nombre de usuario sólo cuando se inicia sesión en la interfaz basada en web del iDRAC6, escriba el siguiente comando:

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName -i <índice>
   ```

   Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

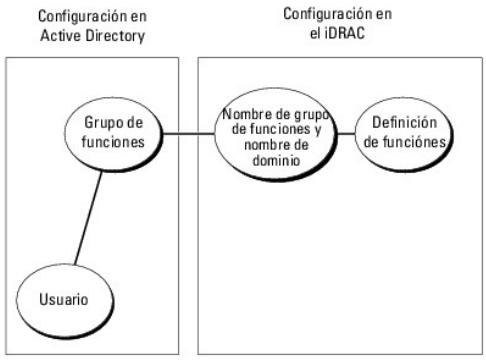
Consulte "Uso de Active Directory para iniciar sesión en el iDRAC6" para obtener información sobre dominios de usuario.

5. Presione **Entrar** para completar la configuración de Active Directory con esquema ampliado.

Generalidades del esquema estándar de Active Directory

Como se muestra en figura 6-3, el uso del esquema estándar para la integración de Active Directory requiere configuración tanto en Active Directory como en iDRAC6.

Figura 6-3. Configuración del iDRAC6 con Microsoft Active Directory y esquema estándar



En Active Directory, se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso al iDRAC6 será miembro del grupo de funciones. Para que este usuario tenga acceso a una tarjeta del iDRAC6 específica, es necesario configurar el nombre del grupo de funciones y el nombre de dominio en esa tarjeta del iDRAC6. A diferencia de la solución de esquema ampliado, la función y el nivel de privilegios se definen en cada tarjeta del iDRAC6 y no en Active Directory. En cada iDRAC6, pueden configurarse y definirse hasta cinco grupos de funciones. La tabla 6-9 muestra los privilegios predeterminados del grupo de funciones.

Tabla 6-9. Privilegios predeterminados del grupo de funciones

Grupos de funciones	Nivel predeterminado de privilegios	Permisos concedidos	Máscara de bits
Grupo de funciones 1	Administrador	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**, **Ejecutar comandos de diagnóstico**	0x000001ff
Grupo de funciones 2	Operador:	**Iniciar sesión en el iDRAC**, **Configurar el iDRAC, Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas, Ejecutar comandos de diagnóstico**	0x000000f9
Grupo de funciones 3	Sólo lectura	Inicio de sesión en iDRAC	0x00000001
Grupo de funciones 4	Ninguno	Sin permisos asignados	0x00000000
Grupo de funciones 5	Ninguno	Sin permisos asignados	0x00000000

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

Casos de dominio único y dominio múltiple

Si todos los usuarios y los grupos de funciones conectados, así como los grupos anidados, están en el mismo dominio, deben configurarse en el iDRAC6 sólo las direcciones de dominio de los controladores. En este caso de dominio único, se admiten todos los tipos de grupos.

Si todos los usuarios y los grupos de funciones conectados, o cualquiera de los grupos anidados, son de múltiples dominios, deben configurarse en el iDRAC6 las direcciones del servidor de Catálogo global. En este caso de dominio múltiple, todos los grupos de función y grupos anidados, si los hubiera, deben ser del tipo Grupo universal.

Configuración de Active Directory con esquema estándar para acceder al iDRAC6

Debe realizar los pasos siguientes para configurar Active Directory antes de que los usuarios de Active Directory puedan acceder al iDRAC6:

1. En un servidor de Active Directory (controlador de dominio), abra el **complemento de usuarios y equipos de Active Directory.**

2. Cree un grupo o seleccione un grupo existente. Los nombres del grupo y de este dominio deben configurarse en el iDRAC6 por medio de la interfaz basada en web o por medio de RACADM (consulte "Configurar Active Directory con esquema estándar con la interfaz basada en web del iDRAC6" o

"Configuración de Active Directory con esquema estándar vía RACADM").

3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para acceder al iDRAC6.

Configurar Active Directory con esquema estándar con la interfaz basada en web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz Web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**.
4. Haga clic en la ficha **Seguridad de la red** y luego haga clic en **Active Directory**.

   Aparece la pantalla **Configuración y administración de Active Directory**.
5. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

   Aparece la pantalla **Paso 1 de 4 Configuración y administración de Active Directory**.
6. En **Configuración de certificados**, seleccione **Activar Active Directory**.
7. En **Cargar un certificado de CA de Active Directory**, escriba la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado y haga clic en **Cargar.**

   NOTA: Debe escribir la ruta completa de acceso al archivo, que incluye la ruta completa de acceso y el nombre y la extensión completos del archivo.

   La información del certificado para el certificado de CA de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.
8. Database (Base de datos personalizada). Haga clic en **Siguiente**.

   Aparece la pantalla **Paso 2 de 4 Configuración y administración de Active Directory**.
9. Seleccione la casilla de marcación **Activar Active Directory.**
10. Haga clic en **Agregar** para ingresar el nombre de dominio de usuario en el campo de texto y luego haga clic en **Aceptar**.
11. En el campo **Tiempo de espera,** ingrese la cantidad de segundos que desea que el iDRAC6 aguarde para las respuestas de Active Directory. El valor predeterminado es 120 segundos.
12. Ingrese la **Dirección de servidor del controlador de dominio**. Puede ingresar hasta tres servidores Active Directory para procesar los inicios de sesión, pero debe configurar al menos un servidor. Para hacerlo, ingrese la dirección IP o el nombre de dominio completo (FQDN). iDRAC6 intenta conectarse a cada servidor configurado hasta establecer una conexión.
13. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 3 de 4 Configuración y administración de Active Directory**.
14. En **Selección del esquema**, seleccione la casilla **Esquema estándar.**
15. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 4a de 4 Configuración y administración de Active Directory**.
16. En **Configuración de esquema estándar**, ingrese las direcciones de servidor de Catálogo global.

    NOTA: Sólo es necesario el servidor de Catálogo global para el esquema estándar cuando las cuentas de usuario y los grupos de funciones se encuentran en dominios diferentes. En el caso de este dominio múltiple, sólo se puede utilizar el Grupo universal.
17. Haga clic en un botón de **Grupo de función** para agregar un grupo de función.

    Aparece la pantalla **Paso 4b de 4 Configurar grupo de funciones 1**.
18. Ingrese el **nombre del grupo.** El nombre del grupo identifica el grupo de funciones en Active Directory asociado con el iDRAC6.
19. Ingrese el **dominio del grupo**. El **Nombre de grupo** es el nombre completo del dominio raíz para el bosque.

20. En la sección **Privilegios del grupo de funciones**, defina los privilegios del grupo. Consulte la tabla 5-11 para obtener información sobre los privilegios de los grupos de funciones.

    NOTA: Si modifica alguno de los permisos, el privilegio del grupo de funciones ya existente (Administrador, Usuario avanzado o Usuario invitado) cambiará al Grupo personalizado o al privilegio de grupo de funciones correspondiente según los permisos que se modifiquen.

21. Haga clic en **Aceptar** para guardar la configuración del grupo de funciones.

    Aparece un diálogo de alerta que le indica que su configuración se ha modificado. Haga clic en Aceptar para volver a la pantalla **Paso 4a de 4, Configuración y administración de Active Directory**.

22. Para agregar un grupo de funciones adicional, repita los pasos paso 17 a paso 21.

23. Haga clic en **Finalizar** y luego haga clic en **Finalizado**.

    Aparece la pantalla **Configuración y administración de Active Directory**. A continuación, debe probar los valores de Active Directory que ha configurado.

24. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configuración de prueba.**

    Aparece la pantalla **Configuración de prueba de Active Directory**.

25. Ingrese su nombre de usuario y contraseña del iDRAC6 y luego haga clic en **Iniciar prueba**.

    Aparecen los resultados y el registro de la prueba. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC6 para admitir el inicio de sesión en Active Directory. Vaya a la página **Acceso remoto→ Configuración→ Red** para configurar los servidores DNS en forma manual o use DHCP para obtener los servidores DNS.

Ha completado la configuración de Active Directory con esquema estándar.

Configuración de Active Directory con esquema estándar vía RACADM

Use los siguientes comandos para configurar la función de Active Directory del iDRAC6 con esquema estándar por medio de la CLI de RACADM en lugar de hacerlo mediante la interfaz basada en web.

1. Abra un indicador de comandos y escriba los siguientes comandos de RACADM:

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

   ```
   racadm config -g cfgActiveDirectory -o cfgADType 2
   ```

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

   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupDomain <nombre totalmente calificado del dominio>

   racadm config -g cfgStandardSchema -i <índice> -o
   cfgSSADRoleGroupPrivilege <número de la máscara de bits para
   los permisos del usuario específico>

   NOTA: Para obtener los valores del número de máscara de bits, consulte la tabla B-1.

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nombre de dominio completo o dirección IP del controlador de dominio>

   NOTA: Ingrese el FQDN del controlador de dominio, *no* el FQDN del dominio. Por ejemplo, ingrese `nombredeservidor.dell.com` en vez de `dell.com`.

   NOTA: Es necesario configurar al menos una de las 3 direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas hasta lograr una conexión exitosa. En el esquema estándar, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <nombre de dominio completo o dirección IP del controlador de dominio>

   NOTA: Sólo es necesario el servidor de Catálogo global para el esquema estándar cuando las cuentas de usuario y los grupos de funciones se encuentran en dominios diferentes. En el caso de este dominio múltiple, sólo se puede utilizar el Grupo universal.

NOTA: La dirección IP o el FQDN que especifique en este campo debe concordar con el campo **Sujeto** o **Nombre alternativo de sujeto** del certificado de controlador de dominio si tiene activada la validación de certificado.

Si desea desactivar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

En este caso, no es necesario cargar ningún certificado de la Autoridad de certificados (CA).

Si desea aplicar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

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

En este caso, también debe cargar el certificado de CA con el siguiente comando de RACADM:

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

El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "Cómo importar el certificado SSL de firmware del iDRAC6".

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

2. Si DHCP está activado en el iDRAC6 y desea usar el DNS proporcionado por el servidor DHCP, escriba los siguientes comandos de RACADM:

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

3. Si el DHCP está deshabilitado en el iDRAC6 o si desea introducir manualmente la dirección IP de DNS, escriba los siguientes comandos de RACADM:

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

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

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

4. Si desea configurar una lista de dominios de usuario para ingresar el nombre de usuario sólo cuando se inicia sesión en la interfaz basada en web, ingrese el siguiente comando:

```
racadm config -g cfgUserDomain -o cfgUserDomainName -i <índice>
```

Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

Consulte "Uso de Active Directory para iniciar sesión en el iDRAC6" para obtener información sobre dominios de usuario.

Prueba de las configuraciones realizadas

Si desea verificar si su configuración funciona o si desea diagnosticar el problema en caso de errores al iniciar sesión en Active Directory, puede realizar pruebas de la configuración en la interfaz basada en web de iDRAC6.

Al finalizar la configuración en la interfaz basada en web de iDRAC6, haga clic en **Configuración de prueba** en la parte inferior de la pantalla. Deberá ingresar un nombre de usuario de prueba (por ejemplo, nombredeusuario@dominio.com) y una contraseña para realizar la prueba. Según la configuración, completar todos los pasos de la prueba y mostrar los resultados de cada paso puede tardar un tiempo. Aparecerá un registro detallado de la prueba en la parte inferior de la pantalla de resultados.

Si se produce un error en cualquiera de los pasos, observe la información que aparece en el registro de la prueba para identificar el error y su posible solución. Para obtener información sobre los errores más frecuentes, consulte "Preguntas frecuentes."

Si desea efectuar cambios en la configuración, haga clic en la ficha **Active Directory** y modifique la configuración según las instrucciones detalladas.

Activación de SSL en un controlador de dominio

Cuando el iDRAC6 autentifica usuarios con un controlador de dominio de Active Directory, inicia una sesión SSL con el controlador de dominio. En este momento, el controlador de dominio debe publicar un certificado firmado por la autoridad de certificación (CA), cuyo certificado raíz se carga en el iDRAC6. En otras palabras, para que el iDRAC6 pueda autentificarse en *cualquier* controlador de dominio (sin importar si es el controlador de dominio raíz o secundario), el controlador de dominio debe tener un certificado habilitado para SSL firmado por la CA del dominio.

Si va a usar la Entidad emisora de certificados raíz de Microsoft para asignar *automáticamente* todos los controladores de dominio a un certificado SSL, realice los pasos siguientes para activar el SSL en cada controlador de dominio:

1. Active SSL en cada uno de los controladores de dominio mediante la instalación del certificado SSL para cada controlador.
   a. Haga clic en **Inicio**→ **Herramientas administrativas**→ **Política de seguridad del dominio**.
   b. Amplíe la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.
   c. En el **Asistente para instalación de solicitud de certificados automática**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.
   d. Haga clic en **Siguiente** y luego en **Terminar**.

Exportación del certificado de CA del controlador de dominio raíz a iDRAC6

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

NOTA: Si está utilizando una CA independiente, los siguientes pasos pueden presentar diferencias.

1. Localice el controlador de dominio que ejecuta el servicio de CA de Microsoft Enterprise.
2. Haga clic en **Inicio**→**Ejecutar**.
3. En el campo **Ejecutar**, escriba `mmc` y haga clic en **Aceptar**.
4. En la ventana **Consola 1** (MMC), haga clic en **Archivo (**o **Consola** en sistemas Windows 2000) y seleccione **Agregar/quitar complemento**.
5. En la ventana **Agregar o quitar complemento**, haga clic en **Agregar**.
6. En la ventana **Complemento independiente**, seleccione **Certificados** y haga clic en **Agregar**.
7. Seleccione la cuenta **Equipo** y haga clic en **Siguiente**.
8. Seleccione **Equipo local** y haga clic en **Terminar**.
9. Haga clic en **Aceptar**.
10. En la ventana **Consola 1,** amplíe la carpeta **Certificados,** amplíe la carpeta **Personal** y haga clic en la carpeta **Certificados**.
11. Ubique el certificado de CA raíz y haga clic en él con el botón derecho del ratón, seleccione **Todas las tareas** y haga clic en **Exportar...**
12. En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.
13. Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.
14. Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.
15. Cargue el certificado que guardó en el paso paso 14en el iDRAC6.

    Para cargar el certificado por medio de RACADM, consulte "Configuración de Active Directory con esquema estándar vía RACADM".

    Para cargar el certificado mediante la interfaz basada en web, consulte "Configurar Active Directory con esquema estándar con la interfaz basada en web del iDRAC6".

Cómo importar el certificado SSL de firmware del iDRAC6

NOTA: Si el servidor de Active Directory está configurado para autentificar el cliente durante una fase de inicialización de sesión SSL, deberá cargar también el certificado de servidor del iDRAC6 en el controlador de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autenticación de cliente durante la fase de inicialización de una sesión SSL.

Use el siguiente procedimiento para importar el certificado SSL de firmware del iDRAC6 a todas las listas de certificados confiables del controlador de dominio.

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

NOTA: Si el certificado SSL de firmware del iDRAC6 está firmado por una CA reconocida y dicho certificado ya se encuentra en la lista de Autoridades de certificación de raíz confiables del controlador de dominio, no es necesario realizar los pasos detallados en esta sección.

El certificado SSL del iDRAC6 es el certificado idéntico que se usa para el servidor web del iDRAC6. Todos los controladores del iDRAC6 se envían con un certificado predeterminado firmado automáticamente.

Para descargar el certificado SSL del iDRAC6, ejecute el siguiente comando de RACADM:

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

1. En el controlador del dominio, abra una ventana **Consola de MMC** y seleccione **Certificados** → **Autoridades de certificación de raíz confiables**.
2. Haga clic con el botón derecho del mouse en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.
3. Haga clic en **Siguiente** y desplácese al archivo de certificado SSL.
4. Instale el certificado SSL del iDRAC6 en la lista de **Autoridades de certificación de raíz confiables** de cada controlador de dominio.

Si ha instalado su propio certificado, asegúrese que la CA que firma su certificado esté en la lista **Autoridad de certificación de raíz confiable**. Si la autoridad no está en la lista, debe instalarla en todos los controladores de dominio.

5. Haga clic en **Siguiente** y seleccione si desea que Windows seleccione automáticamente el almacén de certificados basándose en el tipo de certificado, o desplácese a un almacén de su elección.

6. Haga clic en **Terminar** y luego en **Aceptar**.

Uso de Active Directory para iniciar sesión en el iDRAC6

Puede utilizar Active Directory para iniciar sesión en el iDRAC6 mediante uno de los siguientes métodos:

- Interfaz basada en web
- RACADM local
- SSH o consola Telnet para la CLI de SM-CLP

La sintaxis de inicio de sesión la misma para los tres métodos:

<nombre_de_usuario@dominio>

O bien:

*<dominio>**<nombre_de_usuario>* o *<dominio>*/*<nombre_de_usuario>*

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

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

NOTA: No se pueden especificar nombres de dominio NetBIOS, como *"América"*, porque estos nombres no se pueden resolver.

Si inicia sesión en la interfaz basada en web y ha configurado dominios de usuario, la pantalla de inicio de sesión de la interfaz basada en web brindará un menú desplegable de todos los dominios de usuario para que seleccione el deseado. Si selecciona un dominio de usuario del menú desplegable, sólo debe ingresar el nombre de usuario. Aun si selecciona **Este iDRAC**, podrá iniciar sesión como usuario de Active Directory si utiliza la sintaxis de inicio de sesión descripta más arriba en "Uso de Active Directory para iniciar sesión en el iDRAC6."

Preguntas frecuentes

Problemas de inicio de sesión en Active Directory

No puedo iniciar sesión en Active Directory, ¿qué debo hacer?

iDRAC6 proporciona una herramienta de diagnóstico en la interfaz basada en web.

1. Inicie sesión como usuario local con privilegios de administrador en la interfaz basada en web.

2. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**.

3. Haga clic en la ficha **Red/Seguridad** y luego haga clic en la subficha **Active Directory.**

   Aparece la pantalla **Configuración y administración de Active Directory**.

4. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configuración de prueba.**

   Aparece la pantalla **Configuración de prueba de Active Directory**.

5. Ingrese un nombre de usuario y una contraseña de prueba y luego haga clic en **Iniciar prueba**.

   iDRAC6 ejecuta la prueba paso a paso y muestra el resultado de cada paso. iDRAC6 también registra el resultado detallado de la prueba para ayudarlo a resolver problemas.

   Si los problemas persisten:

   a. En la pantalla **Configuración de prueba**, haga clic en la subficha **Active Directory** para volver a la pantalla **Configuración y administración de Active Directory**.

   b. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

c. Cambie su configuración de usuario y ejecute la prueba nuevamente hasta que el usuario de prueba apruebe el paso de autorización.

Activé la validación del certificado, pero no puedo iniciar sesión en Active Directory. Ejecuté los diagnósticos de la GUI y los resultados de la prueba muestran el siguiente mensaje de error:

ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been 144 Using iDRAC6 With Microsoft Active Directory uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.

(ERROR: No se puede establecer conexión con el servidor LDAP, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:error en la validación del certificado: verifique que se ha cargado en el iDRAC el certificado correcto de la Autoridad de certificados (CA). Verifique también si la fecha del iDRAC se encuentra dentro del período válido de los certificados y si la dirección del controlador de dominio configurada en iDRAC concuerda con el sujeto del certificado del servidor de directorio.)

¿Cuál puede ser el problema y cómo lo soluciono?

Si la validación del certificado está activada, iDRAC6 utiliza el certificado de CA cargado para verificar el certificado del servidor de directorio cuando iDRAC6 establece la conexión SSL con el servidor de directorio. Los motivos más frecuentes de error en la validación del certificado son:

- La fecha del iDRAC6 no se encuentra dentro del período válido del certificado del servidor o del certificado de CA. Verifique el tiempo del iDRAC6 y el período válido de su certificado.
- Las direcciones del controlador de dominio configuradas en el iDRAC6 no concuerdan con el sujeto o con el nombre alternativo del sujeto del certificado del servidor de directorio.
  - Si está usando una dirección IP, consulte "Estoy usando una dirección IP para una dirección de controlador de dominio y no puedo validar el certificado. ¿Cuál es el problema?".
  - Si utiliza un FQDN, asegúrese de estar utilizando el FQDN del controlador de dominio y no el dominio. Por ejemplo, use nombredeservidor.ejemplo.com y *no* ejemplo.com.

¿Qué debo verificar si no puedo iniciar sesión en iDRAC6 con Active Directory?

En primer lugar, diagnostique el problema con la función Configuración de prueba. Para obtener instrucciones, consulte "No puedo iniciar sesión en Active Directory, ¿qué debo hacer?"

Luego, solucione el problema detallado en el resultado de la prueba. Para obtener información adicional, consulte "Prueba de las configuraciones realizadas".

Los problemas más frecuentes se explican en esta sección. Sin embargo, en general, debe verificar lo siguiente:

1. Asegúrese de usar el nombre del dominio de usuario correcto durante un inicio de sesión y no el nombre NetBIOS.
2. Si posee una cuenta de usuario del iDRAC6 local, inicie sesión en el iDRAC6 con las credenciales locales.
3. Compruebe la siguiente configuración:
   a. Diríjase a la pantalla **Configuración y administración de Active Directory**. Seleccione **Sistema→ Acceso Remoto→ iDRAC**, haga clic en la ficha **Red/seguridad** y luego haga clic en la subficha **Active Directory**.
   b. Asegúrese de que la casilla **Active Directory Activado** esté seleccionada.
   c. Si activó la validación del certificado, asegúrese de haber cargado el certificado correcto de CA raíz de Active Directory en iDRAC6. El certificado aparece en el área **Certificado de CA de Active Directory**. Asegúrese de que el tiempo del iDRAC6 se encuentre dentro del período de validez del certificado de CA.
   d. Si está utilizando el esquema ampliado, asegúrese de que el Nombre del **iDRAC** y el Nombre de dominio del **iDRAC** coincidan con la configuración del entorno de Active Directory.

      Si está utilizando el esquema ampliado, asegúrese de que el **Nombre del grupo** y el **Nombre del dominio del grupo** coincidan con la configuración del entorno de Active Directory.
   e. Diríjase a la pantalla Configuración de red. Seleccione **Sistema→Acceso remoto→ iDRAC y** luego haga clic en **Red/ Seguridad.** Compruebe que la configuración de DNS sea correcta.
   f. Verifique los certificados de controlador de dominio SSL para asegurarse de que el tiempo del iDRAC6 está dentro del plazo de vigencia del certificado.

Validación del certificado de Active Directory

Estoy usando una dirección IP para una dirección de controlador de dominio y no puedo validar el certificado. ¿Cuál es el problema?

Verifique el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio. Generalmente, Active Directory utiliza el nombre de host, no la dirección IP, del controlador de dominio en el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio. Puede solucionar el problema por medio de estas acciones:

- Configure el nombre del host (FQDN) del controlador de dominio como las *direcciones de controlador de dominio* en el iDRAC6 para que coincidan con el Sujeto o el Nombre alternativo de sujeto del certificado del servidor.
- Vuelva a emitir el certificado del servidor de forma tal que use una dirección IP en el campo Sujeto o Nombre alternativo de sujeto que concuerde con la dirección IP configurada en el iDRAC6.
- Desactive la validación de certificado si prefiere confiar en este controlador de dominio sin validación de certificado durante el enlace con SSL.

¿Por qué iDRAC6 activa la validación del certificado de forma predeterminada?

iDRAC6 aplica fuertes medios de seguridad para asegurar la identidad del controlador de dominio al que se conecta iDRAC6. Sin la validación de certificados, un pirata informático podría falsificar un controlador de dominio y controlar la conexión SSL. Si decide confiar en todos los controladores de dominio en su barrera de seguridad sin la validación de certificados, puede desactivarla por medio de la GUI o CLI.

Esquema ampliado y esquema estándar

Estoy usando un esquema ampliado en un entorno de dominio múltiple. ¿Cómo configuro las direcciones de controlador de dominio?

Use el nombre del host (FQDN) o la dirección IP de los controladores de dominio donde reside el objeto iDRAC6.

¿Necesito configurar una dirección de Catálogo global?

Si está utilizando un esquema ampliado, no puede configurar direcciones de catálogo global, ya que no se usan con esquema ampliado.

Si está utilizando un esquema estándar, y los usuarios y grupos de funciones pertenecen a dominios distintos, debe configurar las direcciones de catálogo global. En este caso, sólo puede usar Grupo universal.

Si está utilizando un esquema estándar, y todos los usuarios y grupos de funciones se encuentran en el mismo dominio, no es necesario configurar direcciones de catálogo global.

¿Cómo funciona la consulta del esquema estándar?

iDRAC6 se conecta primero a las direcciones de controlador de dominio configuradas. Si tanto el usuario como el grupo de funciones residen en ese dominio, los privilegios se guardan.

Si se configuran direcciones de controlador global, iDRAC6 continúa consultando el Catálogo global. Si se recuperan privilegios adicionales del Catálogo global, estos privilegios se acumulan.

Varios

¿iDRAC6 siempre usa LDAP a través de SSL?

Sí Todo el transporte se realiza mediante el puerto seguro 636 ó 3269.

Durante la *configuración de prueba*, iDRAC6 efectúa una CONEXIÓN A LDAP sólo para ayudar a aislar el problema, pero no se vincula a LDAP con una conexión insegura.

¿iDRAC6 es compatible con el nombre NetBIOS?

No en esta versión.

Regresar a la página de contenido

Regresar a la página de contenido

Visualización de la configuración y la condición del servidor administrado

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Resumen del sistema

Haga clic en **Sistema**→ **Propiedades**→ **Resumen** para obtener información acerca del Gabinete del sistema principal y el Integrated Dell Remote Access Controller.

Gabinete del sistema principal

Información del sistema

Esta sección de la interfaz web del iDRAC6 suministra la siguiente información básica acerca del servidor administrado:

- Descripción: el número de modelo o el nombre del servidor administrado.
- Versión del BIOS: el número de versión del BIOS del servidor administrado.
- Etiqueta de servicio: el número de etiqueta de servicio del servidor administrado.
- Nombre del host: el nombre del host DNS asociado con el servidor administrado.
- Nombre del sistema operativo: el nombre del sistema operativo instalado en el servidor administrado.

Tarjeta intermedia E/S

Esta sección de la interfaz web del iDRAC6 brinda la siguiente información acerca de las tarjetas intermedias de E/S instaladas en el servidor administrado:

- Conexión: presenta una lista de todas las tarjetas intermedias de E/S instaladas en el servidor administrado.
- Tipo de tarjeta: el tipo físico de tarjeta/conexión intermedia instalada.
- Nombre del modelo: el número, tipo o descripción del modelo de la(s) tarjeta(s) intermedia(s) instalada(s).

Tarjeta de almacenamiento integrada

Esta sección de la interfaz web del iDRAC6 brinda información acerca de la tarjeta integrada de controlador de almacenamiento que se encuentra instalada en el servidor administrado:

- Tipo de tarjeta: muestra el nombre del modelo de la tarjeta de almacenamiento instalada.

Autorecuperación

Esta sección de la interfaz web del iDRAC6 detalla el modo de operación actual de la función de autorrecuperación del servidor administrado según la configuración de Open Manage Server Administrator:

- Acción de recuperación: acción a realizar cuando se detecta una falla o *bloqueo* en el sistema. Las acciones disponibles son **Ninguna acción**, **Restablecimiento forzado**, **Apagar** o **Ciclo de encendido**.
- Cuenta regresiva inicial: la cantidad de tiempo (en segundos) después de la detección de un bloqueo de sistema en que el iDRAC6 realiza una acción de recuperación.
- Cuenta regresiva actual: el valor actual (en segundos) del temporizador .

Integrated Dell Remote Access Controller 6 - Enterprise

Información del iDRAC6

Esta sección de la interfaz web del iDRAC6 suministra la siguiente información acerca del iDRAC6:

- Fecha/hora: la fecha y hora actuales (del momento de la última actualización de la página) del iDRAC6.
- Versión del firmware: la versión actual del firmware del iDRAC6 instalada en el servidor administrado.
- Actualización del firmware: la fecha y hora de la última actualización exitosa del firmware del iDRAC6.
- Versión del hardware: el número de versión del plano primario (placa de circuito) del servidor administrado.
- Dirección IP: la dirección IP asociada con el iDRAC6 (no el servidor administrado)
- Puerta de enlace: la dirección IP de la puerta de enlace de red configurada para el iDRAC6.
- Máscara de subred: la máscara de subred TCP/IP configurada para el iDRAC6.
- Dirección MAC: la dirección MAC asociada con el controlador de interfaz de red de LOM (LAN de la placa base) del iDRAC6.
- DHCP activado: activado si el iDRAC6 está configurado para tomar su dirección IP e información asociada de un servidor DHCP.
- Dirección DNS preferida 1: configurada para el servidor DNS primario activo actual.
- Dirección DNS alternativa 2: configurada para el servidor DNS alternativo.

NOTA: Esta información también está disponible en **iDRAC**→ **Propiedades**→ **Información iDRAC**.

Resumen WWN/MAC

Haga clic en **Sistema**→ **Propiedades**→ **WWN/MAC** para ver la configuración actual de las tarjetas intermedias E/S y sus redes fabric asociadas. Si la función FlexAddress está activada, las direcciones MAC persistentes asignadas globalmente (asignado al chasis) reemplazarán a los valores de cableado de cada LOM.

Condición del sistema

Haga clic en **Sistema**→ **Propiedades**→ **Condición** para ver información importante acerca de la condición del iDRAC6 y los componentes supervisados por el iDRAC6. La columna **Gravedad** muestra el estado para cada componente. Para obtener una lista de símbolos de estado y su significado, consulte la tabla 17-3. Haga clic en el nombre del componente en la columna **Componente** para obtener información más detallada acerca del componente.

NOTA: La información del componente también puede obtenerse con un clic sobre el nombre del componente en el panel izquierdo de la ventana. Los componentes permanecen visibles en el panel izquierdo independientemente de la ficha/pantalla seleccionada.

iDRAC6

La pantalla de **Información del iDRAC6** presenta una lista de detalles importantes acerca del iDRAC6, como el estado de la condición, el nombre, la revisión del firmware y los parámetros de red. Se puede acceder a los detalles adicionales haciendo clic sobre la ficha correspondiente ubicada en la parte superior de la pantalla.

CMC

La pantalla **CMC** muestra el estado de la condición, la revisión del firmware y la dirección IP del Chassis Management Controller. También puede iniciar la interfaz web del CMC con un clic sobre el botón **Iniciar la interfaz web del CMC**. Consulte la *Guía del usuario del firmware de Chassis Management Controller*.

Baterías

La pantalla **Baterías**muestra el estado y los valores de la batería de tipo botón de la placa de sistema que mantiene el reloj en tiempo real (RTC) y el almacenamiento de los datos de configuración del CMOS del sistema administrado.

Temperaturas

La pantalla **Información de sondas de temperatura** muestra el estado y las lecturas de la sonda de temperatura ambiente integrada. Se muestran los umbrales de temperatura mínima y máxima para *advertencia* o *falla*, junto con el estado de condición actual de la sonda.

Voltajes

La pantalla **Información de sonda de voltaje** muestra el estado y las lecturas de las sondas de voltaje, y suministra información como el estado del riel de voltaje incorporado y los sensores de núcleo de la CPU.

NOTA: Dependiendo del modelo de su servidor, puede que los umbrales de temperatura para los estados *advertencia* o *falla* y/o estado de condición de la sonda no se visualicen.

Supervisión de alimentación

La pantalla **Supervisión de alimentación** permite ver la siguiente información de supervisión y estadísticas de alimentación:

- Supervisión de alimentación: muestra la cantidad de energía que usa (en watts) el servidor según lo informado por el Monitor actual de la placa de sistema.
- Estadísticas de seguimiento de alimentación: muestra la información acerca de la cantidad de alimentación utilizada por el sistema desde el último restablecimiento de la **Hora inicial de medición.**
- Estadísticas pico: muestra la información acerca de la cantidad pico de alimentación utilizada por el sistema desde el último restablecimiento de la **Hora inicial de medición.**

CPU

La pantalla **Información de la CPU** informa la condición de cada CPU en el servidor administrado. Este estado de condición es un resumen de pruebas individuales térmicas, funcionales y de alimentación.

POST

La pantalla **Código Post** muestra el último código post del sistema (en hexadecimales) antes del inicio del sistema operativo del servidor administrado.

Condiciones diversas

La pantalla **Condiciones diversas** brinda acceso a los siguientes registros del sistema:

- Registros de sucesos del sistema: muestra los sucesos críticos de sistema que se producen en el sistema administrado.
- Código Post: muestra el último código post del sistema (en hexadecimales) antes del inicio del sistema operativo del servidor administrado.
- Último bloqueo: muestra la pantalla y la hora de bloqueo más recientes.
- Captura de inicio: brinda una reproducción de las últimas tres pantallas de inicio.

NOTA: Esta información también está disponible en **Sistema→ Propiedades→ Registros**.

Regresar a la página de contenido

Regresar a la página de contenido

Supervisión y administración de alimentación

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Los sistemas Dell™ PowerEdge™ traen muchas características nuevas y mejoradas de administración de alimentación del sistema. El diseño de toda la plataforma, desde el hardware al firmware hasta el software de administración de sistema, está orientado a la eficacia energética, y a la supervisión y administración de la alimentación.

Los sistemas PowerEdge proporcionan muchas funciones para supervisar y administrar la alimentación.

- **Supervisión de alimentación:** el iDRAC6 recopila un historial de mediciones energéticas y calcula promedios de ejecución, picos, y situaciones similares. Con la interfaz basada en web del iDRAC6 se puede ver esta información en la pantalla **Supervisión de alimentación**. También puede visualizar esta información en forma de gráficas haciendo un clic en **Mostrar gráfica** en el extremo inferior de la pantalla **Supervisión de alimentación**. Para obtener más información, consulte "Control de alimentación".
- **Presupuesto de alimentación:** durante el inicio, un inventario del sistema permite calcular el presupuesto de alimentación de la configuración actual. Consulte "Supervisión de alimentación" para obtener más información.
- **Control de alimentación:** el iDRAC6 permite realizar varias acciones de administración de alimentación en el sistema administrado de manera remota. Consulte "Control de alimentación" para obtener más información.

Configuración y administración de energía

Se puede usar la interfaz basada en web del iDRAC6 y la interfaz de línea de comandos (CLI) RACADM para administrar y configurar los controles de alimentación en el sistema PowerEdge. Expresamente, usted puede:

- Ver el estado de alimentación del servidor. Consulte "Ver la supervisión de alimentación".
- Ver la información de presupuesto de alimentación del servidor, incluido el potencial consumo de alimentación mínimo y máximo. Consulte "Ver el presupuesto de alimentación".
- Ver el umbral del presupuesto de alimentación del servidor. Consulte "Ver el umbral del presupuesto de alimentación".
- Ejecutar operaciones de control de alimentación en el servidor (por ejemplo, encendido, apagado, reinicio del sistema, ciclo de alimentación). Consulte "Ejecución de operaciones de control de alimentación en el servidor".

Supervisión de alimentación

El iDRAC6 supervisa el consumo de alimentación en los servidores PowerEdge en forma continua. El iDRAC6 calcula los siguientes valores de alimentación y proporciona la información a través de su interfaz basada en web o CLI de RACADM:

- Consumo acumulativo de alimentación
- Alimentación promedio, mínima y máxima
- Consumo de alimentación (también puede verlo en gráficas en la interfaz basada en web)
- Umbrales de presupuesto de alimentación

Ver la supervisión de alimentación

Por medio de la interfaz web

Para ver la información de supervisión de alimentación:

1. Inicie sesión en la interfaz Web del iDRAC6.
2. En el árbol del sistema, seleccione **Supervisión de alimentación**.

   Aparece la pantalla **Supervisión de alimentación**, la cual muestra la siguiente información:

Supervisión de alimentación

- **Estado**: una **marca de verificación verde** indica que el estado de la alimentación es normal, **Alerta** indica que se ha emitido una alerta de advertencia, y **Grave** indica que se ha emitido una alerta de error.

- **Nombre de la sonda**: nivel del sistema de la placa del sistema. La descripción indica que la sonda está supervisada por su ubicación en el sistema.
- **Lectura**: el consumo de energía actual en vatios.

Amperaje

- **Ubicación**: monitor actual de la placa de sistema
- **Lectura**: el consumo de energía actual en amperios.

Estadísticas de seguimiento de alimentación

- Estadística:
  - **La Alimentación acumulada del sistema** muestra el consumo de energía acumulada actual (en KWh) del servidor. El valor representa la energía total utilizada por el sistema. Puede restablecer este valor a 0 al hacer clic en **Restablecer,** ubicada al final de la fila.
  - **La Alimentación pico del sistema** especifica el valor pico del sistema en vatios dentro del intervalo indicado por la **Hora de inicio de medición** y la **Hora actual de medición**. Puede restablecer este valor a 0 al hacer clic en **Restablecer,** ubicada al final de la fila.
  - **Amperaje pico del sistema** especifica el amperaje pico del sistema dentro del intervalo indicado por la **Hora de inicio de medición** y la **Hora actual de medición**. Puede restablecer este valor a 0 al hacer clic en **Restablecer,** ubicada al final de la fila.
- **La Hora de inicio de medición** muestra la fecha y la hora registradas cuando se borró por última vez el valor de consumo de energía del sistema y comenzó el nuevo ciclo de mediciones. Para las estadísticas de **Alimentación acumulada del sistema**, **Amperaje pico del sistema** y **Alimentación pico del sistema**, puede restablecer cada uno de los valores a 0 al hacer clic en **Restablecer,** ubicada al fin de la lista; sin embargo, persistirá en caso de reinicio del sistema o de una operación de sustitución tras error del CMC.
- **La Hora actual de medición** para la **Alimentación acumulada del sistema** muestra la fecha y hora en las que se calculó el consumo de energía del sistema para su visualización. Para el **Amperaje pico del sistema** y la **Alimentación pico del sistema**, los campos de **Hora pico** muestran la hora en que tuvieron lugar dichos picos.
- **Lectura**: la cantidad de energía (en KWh) utilizada desde el inicio del contador.

NOTA: Las Estadísticas de seguimiento de alimentación se mantienen en caso de restablecimientos del sistema y reflejan toda la actividad en el intervalo entre las horas de Inicio y Finalización establecidas. El botón **Restablecer picos máximos** restablecerá los valores estadísticos de picos. En la tabla siguiente, la información de Consumo de alimentación no se mantiene en caso de restablecimiento del sistema por lo que se restablecerá a los valores pico estadísticos. Los valores de alimentación que se muestran son promedios acumulados en el intervalo de tiempo respectivo (minuto, hora, día y semana previos). Debido a que los intervalos de tiempo de inicio y fin pueden ser distintos de aquellos de las estadísticas de seguimiento de alimentación, los valores de alimentación pico (picos máximos en vatios en comparación con consumo máximo de alimentación) pueden ser distintos.

Consumo de alimentación

- **Consumo de alimentación promedio**: promedio sobre minuto, hora, día y mes anteriores.
- **Consumo de alimentación máximo y Consumo de alimentación mínimo:** el consumo de alimentación máximo y mínimo observado dentro de un intervalo de tiempo determinado.
- **Fecha y hora de alimentación máxima** y **Fecha y hora de alimentación mínima**: el momento (minuto, hora, día y semana) en el que ocurrió el consumo de alimentación mínimo y máximo.

Mostrar gráfica

Haga clic en **Mostrar gráfica** para ver las gráficas que muestran el consumo de energía del iDRAC6 en vatios durante la última hora, las últimas 24 horas, tres días y una semana. Use el menú desplegable que se encuentra por encima del gráfico para seleccionar el período de tiempo.

NOTA: Cada uno de los puntos de información de la gráfica representa el promedio de lecturas en un lapso de 5 minutos. Como resultado, es posible que la gráfica no refleje fluctuaciones breves de alimentación ni tampoco el consumo actual.

[Presupuesto de alimentación]

El iDRAC6 puede estar configurado para aplicar los límites mínimos y máximos del umbral de alimentación, según lo establecido en el CMC, para la configuración actual del sistema. La pantalla **Presupuesto de alimentación** muestra los límites de los umbrales de alimentación, los cuales cubren el rango de consumo de alimentación de CA que presenta al centro de datos un sistema con umbrales con una gran carga de trabajo. Estos límites no pueden configurarse.

Ver el presupuesto de alimentación

El servidor proporciona una descripción general del estado del presupuesto de alimentación del subsistema de alimentación en la pantalla **Información de presupuesto de alimentación**.

Por medio de la interfaz web

NOTA: Para realizar acciones de administración de alimentación, se debe contar con privilegios de **Administrador**.

1. Inicie sesión en la interfaz basada en web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema.**
3. Haga clic en la ficha **Administración de alimentación** y luego en **Presupuesto de alimentación**.

   Aparecerá la pantalla **Información del presupuesto de alimentación**.

La tabla **Información sobre el presupuesto de alimentación** muestra los límites mínimo y máximo de los umbrales de alimentación para la configuración actual del sistema. Estos cubren el rango de consumo de alimentación de CA que presenta al centro de datos un sistema con umbrales con una gran carga de trabajo.

- **El Consumo de alimentación potencial mínimo** representa el valor más bajo del Umbral de presupuesto de alimentación.
- **El Consumo de alimentación potencial máximo** representa el valor más alto del Umbral de presupuesto de alimentación. Este valor es también el consumo de alimentación máximo absoluto de la configuración actual del sistema.

Uso de RACADM

En un nodo administrado, abra una interfaz de línea de comandos y escriba:

```
racadm getconfig -g cfgServerPower
```

NOTA: Para obtener más información acerca de cfgServerPower, incluso los detalles de mensajes de salida, consulte "cfgServerPower".

Ver el umbral del presupuesto de alimentación

El umbral del presupuesto de alimentación, si está activado, aplica los límites de alimentación para el sistema. El rendimiento del sistema se ajusta en forma dinámica a fin de mantener el consumo de alimentación cerca del umbral determinado.

NOTA: El umbral del presupuesto de alimentación es de sólo lectura. No es posible activarlo o configurarlo en el iDRAC6.

El consumo de alimentación real puede ser menor en cargas de trabajo más livianas y puede exceder el umbral de forma momentánea hasta completar los ajustes de rendimiento.

Uso de la interfaz basada en web

1. Inicie sesión en la interfaz basada en web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema.**
3. Haga clic en la ficha **Administración de alimentación** y luego en **Presupuesto de alimentación**.

   Aparecerá la pantalla **Información del presupuesto de alimentación**.

4. Haga clic en **Umbral del presupuesto de alimentación**.

La tabla del **Umbral del presupuesto de alimentación** muestra información sobre el límite de alimentación del sistema:

- **Activado** indica si el sistema aplica el umbral del presupuesto de alimentación.
- **Umbral en vatios** y **Umbral en BTU/h** muestra el límite en vatios y BTU/h, respectivamente.
- **Porcentaje del umbral** muestra el porcentaje del rango de alimentación.

Uso de RACADM

En un nodo administrado, abra una interfaz de línea de comandos y escriba:

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts <valor máximo de alimentación expresado en vatios>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr <valor máximo de alimentación expresado en BTU/h>

racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts <valor máximo de alimentación expresado en porcentajes>
```

NOTA: Para obtener más información acerca de cfgServerPower, incluso los detalles de mensajes de salida, consulte "cfgServerPower".

Control de alimentación

El iDRAC6 le permite realizar las siguientes acciones en forma remota: encendido, reinicio, apagado ordenado, interrupción no enmascarable (NMI) o ciclo de encendido. Use la pantalla **Control de alimentación** para realizar un apagado ordenado por medio del sistema operativo al reiniciar, encender y apagar el sistema.

Ejecución de operaciones de control de alimentación en el servidor

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de control de chasis**.

El iDRAC6 le permite realizar en forma remota las siguientes acciones: encendido, reinicio, apagado ordenado, interrupción no enmascarable (NMI) o ciclo de encendido.

Por medio de la interfaz web

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Seleccione **Sistema** en el árbol del sistema.
3. Haga clic en la ficha **Power Management** (Administración de energía).

   Aparece la pantalla **Control de alimentación**.
4. Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en su botón de radio:
   - **Encender el sistema:** enciende el servidor (equivalente a presionar el botón de encendido cuando el servidor está apagado). Esta opción se desactivará si el sistema ya está encendido.
   - **Apagar el sistema:** apaga el servidor. Esta acción se desactivará si el sistema ya está apagado.
   - **NMI (Interrupción no enmascarable)** genera una NMI para detener el sistema. Un NMI envía una interrupción de alto nivel al sistema operativo, lo cual hace que el sistema detenga la operación para permitir la ejecución de actividades fundamentales de diagnóstico o solución de problemas.
   - **Apagado ordenado:** intenta cerrar de manera estructurada el sistema operativo y luego apaga el sistema. Para efectuar el apagado ordenado, es necesario contar con un sistema operativo con ACPI (Interfaz de energía y configuración avanzada), lo cual permite la administración de la alimentación dirigida por el sistema.
   - **Restablecer el sistema (reinicio mediante sistema operativo):** reinicia el sistema sin apagarlo. Esta acción se desactivará si el sistema ya está apagado.
   - **Ciclo de encendido del sistema** (inicio en frío) **apaga el sistema y luego lo reinicia**. Esta acción se desactivará si el sistema ya está apagado.
5. Haga clic en **Aplicar**.

   Aparece un cuadro de diálogo que le solicita confirmación.
6. Haga clic en **Aceptar** para ejecutar la acción de administración de alimentación que ha seleccionado.

Uso de RACADM

Abra un nodo administrado y abra una consola de texto en la interfaz de línea de comandos al servidor, luego inicie sesión y escriba:

```
racadm serveraction <acción>
```

donde `<acción>` es `powerup`, `powerdown`, `powercycle`, `hardreset` o `powerstatus`.

NOTA: Para obtener más información acerca de acciones del servidor, incluso los detalles de mensajes de salida, consulte "serveraction".

Regresar a la página de contenido

Regresar a la página de contenido

Configuración y uso de la comunicación en serie en la LAN

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

La comunicación en serie en la LAN (SOL) es una función de IPMI que permite que los datos de consola basados en texto de un servidor administrado, en lugar de enviarse al puerto de E/S serie como se haría en forma tradicional, se envíen a través de la red específica de administración Ethernet fuera de banda del iDRAC. La consola fuera de banda de SOL permite que los administradores de sistemas administren de forma remota la consola de texto del servidor de hoja desde cualquier lugar con acceso a la red. Los beneficios de SOL son los siguientes:

- Acceder de forma remota a los sistemas operativos sin agotar el tiempo de espera.
- Realizar diagnósticos de sistemas host en servicios de administración de emergencia (EMS) o la consola administrativa especial (SAC) para Windows o un shell de Linux.
- Ver el progreso de un servidor de hoja durante la autoprueba de encendido (POST) y reconfigurar el programa de configuración del BIOS (mientras se dirige a un puerto serie).

Activación de la comunicación en serie en la LAN en el BIOS

Para configurar un servidor para la comunicación en serie en la LAN, es necesario llevar a cabo los pasos de configuración que se describen detalladamente a continuación.

1. Configurar la comunicación en serie en la LAN en el BIOS (opción deshabilitada de manera predeterminada)
2. Configurar el iDRAC6 para la comunicación en serie en la LAN
3. Seleccionar un método para inicializar la comunicación en serie en la LAN (SSH, Telnet, proxy SOL o IPMITool)
4. Configurar el sistema operativo para SOL

De manera predeterminada, la comunicación en serie está **desactivada** en el BIOS. Para redirigir los datos de texto de la consola a la comunicación en serie en la LAN, debe activar la redirección de consola a través de COM1. Para cambiar el valor en el BIOS, realice los pasos a continuación:

1. Inicie el servidor administrado.
2. Presione <F2> para acceder a la utilidad de configuración del BIOS durante la autoprueba de encendido.
3. Desplácese hacia abajo hasta llegar a Comunicación serie y presione <Entrar>.

   En la ventana emergente, la lista de comunicaciones en serie aparece con las siguientes opciones:

   - Luz apagada
   - Encendido sin redirección de consola
   - Encendido con redirección de consola a través de COM1

   Utilice las teclas de flecha para recorrer las opciones.
4. Asegúrese de que la opción **Encendido con redirección de consola a través de COM1** esté activada.
5. Verifique que el valor de **Velocidad en baudios libre de fallas** sea idéntico a la velocidad en baudios de SOL configurada en el iDRAC. El valor predeterminado en ambos casos es 115,2 kbps.
6. Active la opción **Redirección después de inicio** (el valor predeterminado es DESACTIVADA). Esta opción activa la redirección de SOL del BIOS en los reinicios subsecuentes.
7. Guarde los cambios y salga.

   El servidor administrado se reinicia.

Configuración de la comunicación en serie en la LAN en la GUI del iDRAC6

1. Abra la pantalla **Configuración de la comunicación en serie en la LAN** de la siguiente manera: seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**→

Red/Seguridad → **Comunicación en serie en la LAN**.

2. Verifique que la opción **Activar comunicación en serie en la LAN** esté seleccionada (activada). De manera predeterminada, la opción se encuentra activada.

3. Actualice la velocidad en baudios de SOL de IPMI seleccionando un valor en el menú desplegable **Velocidad en baudios**. Las opciones son 19,2 kbps, 57,6 kbps y 115,2 kbps. El valor predeterminado es 115,2.

   NOTA: Asegúrese de que la velocidad en baudios de SOL sea idéntica al valor de la opción Velocidad en baudios a prueba de fallas definida en el BIOS.

4. Haga clic en **Aplicar** si realizó cambios.

Tabla 9-1. Valores de configuración de comunicación en serie en la LAN:

Valor	Descripción
Activar comunicación en serie en la LAN.	Cuando está seleccionada, la casilla indica que la comunicación en serie en la LAN está activada.
Velocidad en baudios	Indica la velocidad de los datos. Seleccione una velocidad de datos de **19,2 kbps**, **57,6 kbps** o **115,2 kbps**.

Tabla 9-2. Botones de configuración de la comunicación en serie en la LAN

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración de la comunicación en serie en la LAN** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **Configuración de la comunicación en serie en la LAN.**
Configuración avanzada	Abre la pantalla **Configuración avanzada de la comunicación en serie en la LAN**.
Aplicar	Proporciona los nuevos valores de configuración asignados mientras se visualiza la pantalla **Configuración de la comunicación en serie en la LAN**.

5. Cambie la configuración en la pantalla **Configuración avanzada**, en caso de ser necesario. Dell recomienda utilizar los valores predeterminados. La sección **Configuración avanzada** le permite ajustar el rendimiento de SOL mediante la modificación de los valores **Intervalo de acumulación de caracteres** y **Umbral de envío de caracteres**. Para obtener un óptimo rendimiento, utilice los valores predeterminados de 10 milisegundos y 250 caracteres respectivamente.

Tabla 9-3. Valores de la pantalla de configuración avanzada de la comunicación en serie en la LAN

Valor	Descripción
Intervalo de acumulación de caracteres	Es la cantidad típica de tiempo que el iDRAC6 espera antes de enviar un paquete de datos parcial de SOL. Este parámetro se expresa en milisegundos y se incrementa en intervalos de 10 milisegundos.
Umbral de envío de caracteres	Indica la cantidad de caracteres por paquete de datos de SOL. Cuando la cantidad de caracteres aceptados por el iDRAC6 es igual o superior al valor de Umbral de envío de caracteres, el iDRAC6 comienza a transmitir de inmediato paquetes de datos de SOL que contienen una cantidad de caracteres igual o inferior a dicho valor. Si un paquete contiene menos caracteres que lo expresado por este valor, se define como un paquete de datos de SOL parcial.

NOTA: Si cambia estos valores por otros menores, la función de redirección de consola de SOL puede reducir su rendimiento. Además, la sesión de SOL debe aguardar para recibir una confirmación por cada paquete antes de enviar el siguiente. En consecuencia, el rendimiento disminuye significativamente.

Tabla 9-4. Botones de configuración avanzada de la comunicación en serie en la LAN

Botón	Descripción
Imprimir	Imprime los valores de la **Configuración avanzada de la comunicación en serie en la LAN** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **Configuración avanzada de la comunicación en serie en la LAN**.
Aplicar	Guarda cualquier configuración nueva asignada mientras se visualiza la pantalla **Configuración avanzada de la comunicación en serie en la LAN**.
Volver a la página de configuración de la comunicación en serie en la LAN	Regresa al usuario a la pantalla **Configuración de la comunicación en serie en la LAN**.

6. Configure SSH/Telnet para SOL en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**→ **Servicios**.

   NOTA: Cada servidor de hoja admite sólo una sesión de SOL activa a través del protocolo Telnet o SSH.

   NOTA: De manera predeterminada, el protocolo SSH está activado. De manera predeterminada, el protocolo Telnet está desactivado.

7. Haga clic en **Servicios** para abrir la pantalla **Configuración de SSH y Telnet**.

   NOTA: Los programas SSH y Telnet proporcionan acceso a través de un sistema remoto.

8. Haga clic en **Activar** en **SSH** o **Telnet** según sea necesario.

9. Haga clic en **Aplicar**.

   NOTA: SSH es el protocolo recomendado debido a sus mejores mecanismos de cifrado y seguridad.

   NOTA: La duración de la sesión de SSH/Telnet puede ser infinita si el valor de límite de tiempo se establece en 0. El valor predeterminado es **1800 segundos**.

10. Active la interfaz fuera de banda del iDRAC6 (IPMI en la LAN). Para ello, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**→ **Red**.

11. Active la opción **IPMI en la LAN** en la sección **Configuración de la LAN IPMI**. De manera predeterminada, la función **IPMI en la LAN** se encuentra desactivada.

12. Haga clic en **Aplicar**.

Uso de la comunicación en serie en la LAN (SOL)

En esta sección se ofrecen diversos métodos para inicializar una sesión de comunicación en serie en la LAN, lo que incluye un programa de Telnet, un cliente SSH, la herramienta IPMItool y el proxy SOL. El propósito de la función de comunicación en serie en la LAN consiste en redirigir el puerto serie del servidor administrado a través del iDRAC6 a la consola de la estación de administración.

Modelo para dirigir la comunicación en serie en la LAN a través de Telnet o SSH

Cliente de Telnet (puerto 23)/ SSH (puerto 22)←→ Conexión WAN←→ Servidor de iDRAC6

La implementación de la función SOL con base en IPMI a través de SSH/Telnet elimina la necesidad de contar con una utilidad adicional ya que la traducción de comunicación en serie a comunicación de red se realiza dentro del iDRAC. La consola de Telnet o SSH que usted utiliza debe ser capaz de interpretar y responder a los datos provenientes del puerto serie del servidor administrado. El puerto serie por lo general se conecta a un shell que emula una terminal ANSI o VT100. La consola en serie se envía automáticamente a la consola de Telnet o SSH. La redirección de la comunicación en serie en la LAN se puede iniciar desde el destino **/system1/soll**.

Consulte "Instalación de clientes Telnet o SSH" para obtener más información sobre cómo usar clientes Telnet y SSH con el iDRAC.

Modelo para proxy SOL

Cliente Telnet (puerto 623) ←→ Conexión WAN ←→ Proxy SOL ←→ Servidor del iDRAC6

Cuando el proxy SOL se comunica con el cliente Telnet en una estación de administración, utiliza el protocolo TCP/IP. No obstante, el proxy SOL se comunica con el iDRAC6 del servidor administrado a través del protocolo RMCP/IPMI/SOL, el cual es un protocolo basado en UDP. Por lo tanto, si la comunicación con el iDRAC6 del sistema administrado desde el proxy SOL se realiza a través de una conexión WAN, es posible que surjan problemas de rendimiento de red. El modelo de uso recomendado es que el proxy SOL y el servidor del iDRAC6 estén en la misma LAN. De esta forma, la estación de administración con el cliente Telnet podrá conectarse al proxy SOL a través de una conexión WAN. En este modelo, el proxy SOL funcionará según se desee.

Modelo para dirigir la comunicación en serie en la LAN a través de IPMItool

IPMItool ←→ Conexión WAN←→ Servidor del iDRAC6

La utilidad SOL basada en IPMI, IPMItool, utiliza el protocolo RMCP+ a través de datagramas UDP con el puerto 623. iDRAC6 requiere que esta conexión RMCP+ esté cifrada. La clave de cifrado (clave KG) debe contener caracteres de valor cero o NULO que puedan configurarse en la GUI web del iDRAC6 o en la utilidad de configuración del iDRAC6. También es posible borrar la clave de cifrado presionando la tecla de retroceso para que el iDRAC6 proporcione caracteres NULOS como la clave de cifrado predeterminada. La ventaja de usar RMCP+ es una mejor autenticación, control de integridad de los datos, cifrado y capacidad para varios tipos de carga. Consulte "Uso de SOL a través de IPMItool" o el sitio web de IPMItool para más información: **http://ipmitool.sourceforge.net/manpage.html**.

Desconexión de una sesión SOL en SM-CLP

Cuando utiliza protocolos SSH o Telnet para acceder a la función en serie en la LAN, en primer lugar se conectará con el servicio SM-CLP del iDRAC y desde allí podrá abrir la sesión SOL con un comando SM-CLP (`start /system1/sol1`). Por lo tanto, los usuarios que desean desconectar una sesión SOL en primer lugar deben finalizar la sesión desde SM-CLP.

Los comandos para desconectar una sesión SOL se centran en la utilidad. Lea esta sección detenidamente. Sólo cuando la sesión SOL haya finalizado por completo, podrá salir de la utilidad.

Cuando esté listo para salir de la redirección de SOL desde SM-CLP, presione <Entrar>, <Esc> y después <t> (presione las teclas en secuencia, una tras otra).

La sesión SOL se cerrará.

NOTA: Si la sesión SOL no se cierra correctamente en la utilidad, no habrá más sesiones disponibles. Para resolver esta situación, hay que eliminar la consola SMASH en la interfaz gráfica web del usuario en **Sistema**→**Acceso remoto**→**iDRAC**→ **Red / Seguridad**→**Sesiones**.

Uso de SOL a través de PuTTY

Para iniciar la comunicación en serie en la LAN desde PuTTY en una estación de administración Windows, siga estos pasos:

NOTA: De ser necesario, puede cambiar el tiempo de espera predeterminado de SSH/Telnet en **Sistema** → **Acceso remoto**→ **iDRAC** → **Red / Seguridad** → **Servicios**.

1. Para conectarse al iDRAC6, ingrese el siguiente comando en el indicador de comandos:

   ```
   putty.exe [-ssh | -telnet] <nombre de inicio de sesión>@<dirección_IP_de_iDRAC> <número de puerto>
   ```

   NOTA: El número de puerto es opcional. Se requiere únicamente cuando se reasigna el número de puerto.

2. Ingrese el siguiente comando en la ventana de SM-CLP para iniciar SOL:

   ```
   start /system1/sol1
   ```

   NOTA: Con esto se conectará al puerto serie del servidor administrado. Los comandos de SM-CLP ya no estarán disponibles para usted. Una vez que haya iniciado la SOL, no podrá regresar a SM-CLP. Deberá salir de la sesión de SOL por medio de la secuencia de comandos que se describe en "Desconexión de una sesión SOL en SM-CLP" e iniciar una nueva para usar SM-CLP.

Uso de la comunicación en serie en la LAN mediante Telnet con Linux

Para iniciar la comunicación en serie en la LAN por medio de Telnet en una estación de administración con Linux, siga estos pasos:

NOTA: De ser necesario, puede cambiar el tiempo de espera predeterminado de Telnet en **Sistema** → **Acceso remoto**→ **iDRAC** → **Red / Seguridad** → **Servicios**.

1. Inicie una ventana de shell.
2. Para conectarse al iDRAC6, ingrese el comando siguiente:

   ```
   telnet <dirección_IP_del_iDRAC>
   ```

   NOTA: Si cambió el número predeterminado de puerto del servicio de Telnet (puerto 23), agregue el número de puerto al final del comando telnet.

3. Ingrese el nombre de usuario y la contraseña del iDRAC para conectarse a SM-CLP del iDRAC6.
4. Ingrese el siguiente comando en la ventana de SM-CLP para iniciar SOL:

   ```
   start /system1/sol1
   ```

5. Para salir de una sesión SOL desde Telnet en Linux, presione <Ctrl>+] (sostenga la tecla control y presione la tecla + y el corchete derecho, luego suelte estas teclas). Aparecerá una petición de Telnet. Escriba `quit` para salir de Telnet.

Uso de la comunicación en serie en la LAN mediante OpenSSH con Linux

OpenSSH es una utilidad de código abierto para usar el protocolo SSH. Para iniciar la comunicación en serie en la LAN desde OpenSSH en una estación de administración Linux, siga estos pasos:

NOTA: De ser necesario, puede cambiar el tiempo de espera predeterminado de SSH en **Sistema** → **Acceso remoto**→ **iDRAC** → **Red / Seguridad** → **Servicios**.

1. Inicie una ventana de shell.
2. Para conectarse al iDRAC6, ingrese el comando siguiente:

   ```
   ssh <dirección_IP_de_iDRAC> -l <nombre de inicio de sesión>
   ```

3. Ingrese el siguiente comando en la ventana de SM-CLP para iniciar SOL:

   ```
   start /system1/sol1
   ```

NOTA: Con esto se conectará al puerto serie del servidor administrado. Los comandos de SM-CLP ya no estarán disponibles para usted. Una vez que haya iniciado la SOL, no podrá regresar a SM-CLP. Debe salir de la sesión SOL (consulte "Desconexión de una sesión SOL en SM-CLP" para cerrar una sesión SOL activa) e inicie una nueva sesión para usar SM-CLP.

Uso de SOL a través de IPMItool

El DVD *Dell Systems Management Tools and Documentation* incluye IPMItool, una herramienta que puede instalarse en diversos sistemas operativos. Para iniciar la comunicación en serie en la LAN con IPMItool en una estación de administración, siga estos pasos:

NOTA: De ser necesario, puede cambiar el límite de tiempo de espera predeterminado de SOL en **Sistema** → **Acceso remoto**→ **iDRAC** → **Red/Seguridad** → **Servicios**.

1. Localice el archivo IPMItool.exe en el directorio correspondiente.

   La ruta de acceso predeterminada para Windows es **C:\Archivos de programa\Dell\SysMgt\bmc**.

2. Asegúrese de que la **Clave de cifrado** contenga sólo ceros en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**→ **Red**→ **Configuración de la LAN IPMI**.

3. Ingrese el siguiente comando en el indicador de comandos de Windows o en la ventana de petición de comandos del shell de Linux para iniciar SOL a través del iDRAC:

   `ipmitool -H <dirección_IP_de_iDRAC> -I lanplus -U <nombre de inicio de sesión> -P <contraseña de inicio de sesión> sol activate`

   Con esto se conectará al puerto serie del servidor administrado.

4. Para salir de una sesión SOL desde IPMItool, presione <~> y <.> (presione las teclas de tilde y punto en secuencia, una después de la otra). La sesión SOL se cerrará.

   NOTA: Si un usuario no finaliza la sesión correctamente, ejecute el siguiente comando para reiniciar el iDRAC. Espere entre 1 y 2 minutos hasta que el iDRAC6 se inicie por completo. Para obtener más información, consulte "Generalidades del subcomando RACADM".

   ```
   racadm racreset
   ```

Ejecución de SOL con el proxy SOL

El proxy SOL es un demonio de Telnet que permite la administración basada en LAN de sistemas remotos con los protocolos de comunicación en serie en la LAN (SOL) e IPMI. Se puede utilizar cualquier aplicación de cliente Telnet estándar, como HyperTerminal en Windows o Telnet en Linux, para acceder a las funciones del demonio. SOL se puede utilizar en el modo ya sea de comando o de menú. El protocolo SOL acoplado a la redirección de consola del BIOS del sistema remoto permite a los administradores ver y cambiar de forma remota la configuración del BIOS del sistema administrado mediante una LAN. También se puede acceder a la consola en serie de Linux y a las interfaces EMS/SAC de Microsoft a través de una LAN mediante SOL.

NOTA: Todas las versiones del sistema operativo Windows incluyen el software de emulación de terminal HyperTerminal. Sin embargo, la versión incluida no proporciona numerosas funciones necesarias durante la redirección de consola. En su lugar, puede utilizar cualquier software de emulación de terminal que admita el modo de emulación VT100 o ANSI. Un ejemplo de un emulador de terminal VT100 o ANSI completo que admite la redirección de consola en el sistema es HyperTerminal Private Edition 6.1 o posterior.

NOTA: Consulte la guía del usuario del sistema para obtener más información sobre la redirección de consola, incluyendo los requisitos de hardware y software, así como instrucciones para configurar sistemas cliente y host que utilicen la redirección de consola.

NOTA: La configuración de HyperTerminal y Telnet debe ser coherente con la configuración del sistema administrado. Por ejemplo, las velocidades en baudios y los modos de terminal deben coincidir.

NOTA: El comando `telnet` de Windows que se ejecuta desde el símbolo del sistema de MS-DOS® admite la emulación de terminal ANSI, y el BIOS debe estar configurado para la emulación ANSI para que todas las pantallas se muestren correctamente.

Antes de usar el proxy SOL

Antes de usar el proxy SOL, consulte la *Guía del usuario de las utilidades del controlador de administración de la placa base* para saber cómo configurar las estaciones de administración. De manera predeterminada, la utilidad de administración de BMC está instalada en el siguiente directorio en los sistemas operativos Windows:

C:\Archivos de programa\Dell\SysMgt\bmc.

El programa de instalación copia los archivos en las siguientes ubicaciones en los sistemas operativos Linux Enterprise:

/etc/init.d/SOLPROXY.cfg

/etc/solproxy.cfg

/usr/sbin/dsm_bmu_solproxy32d

/usr/sbin/solconfig

/usr/sbin/ipmish

Inicio de sesión del proxy SOL

Para Windows 2003

Para iniciar el servicio proxy SOL en un sistema Windows después de la instalación, puede reiniciar el sistema (el proxy SOL se inicia automáticamente después del reinicio). O bien, puede iniciar el servicio proxy SOL manualmente mediante los siguientes pasos:

1. Haga clic con el botón derecho del mouse en **Mi PC** y haga clic en **Administrar**.

   Aparecerá la ventana **Administración del equipo**.

2. Haga clic en **Servicios y aplicaciones** y luego en **Servicios**.

   Los servicios disponibles se muestran a la derecha.

3. Ubique **DSM _BMU_SOLProxy** en la lista de servicios y haga clic con el botón derecho del mouse para iniciar el servicio.

Dependiendo de la consola que utilice, existen distintos pasos para acceder a Proxy SOL. En esta sección, la estación de administración en la que se está ejecutando el proxy SOL se denomina servidor proxy SOL.

Para Linux

Proxy SOL se iniciará automáticamente durante el inicio del sistema. Asimismo, puede acceder al directorio **/etc/init.d** y utilizar los siguientes comandos para administrar el servicio Proxy SOL:

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

Uso de Telnet con el proxy SOL

Esta sección parte de la premisa de que el servicio proxy SOL ya está en funcionamiento en la estación de administración.

Para Windows 2003:

1. Abra una ventana de petición de comandos en la estación de administración.

2. Ingrese el comando `telnet` en la línea de comandos y escriba `localhost` como dirección IP si el servidor proxy SOL se ejecuta en el mismo sistema y el número de puerto que se especificó en la instalación del proxy SOL (el valor predeterminado es 623). Por ejemplo:

   ```
   telnet localhost 623
   ```

Para Linux:

1. Abra un shell de Linux en la estación de administración.

2. Ingrese el comando `telnet` y escriba `localhost` como la dirección IP del servidor proxy SOL y el número de puerto que se especificó en la instalación del proxy SOL (el valor predeterminado es 623). Por ejemplo:

   ```
   telnet localhost 623
   ```

NOTA: Independientemente de que el sistema operativo host sea Windows o Linux, si el servidor proxy SOL se ejecuta en un sistema diferente de la estación de administración, ingrese la dirección IP del servidor proxy SOL en lugar de localhost.

```
telnet <dirección IP del servidor proxy SOL> 623
```

Uso de HyperTerminal con el proxy SOL

1. Desde la estación remota, abra **HyperTerminal.exe**.

2. Elija **TCP IP (Winsock)**.

3. Ingrese la dirección de host `localhost` y el número de puerto 623.

Conexión al BMC del sistema administrado remoto

Después de iniciar correctamente una sesión de proxy SOL, se le presentarán las siguientes opciones:

1. `Connect to the Remote Server's BMC (Conectarse al BMC del servidor remoto)`
2. `Configure the Serial-Over-LAN for the Remote Server (Configurar la comunicación en serie en la LAN para el servidor remoto)`
3. `Activate Console Redirection (Activar la redirección de consola)`
4. `Reboot and Activate Console Redirection (Reiniciar y activar la redirección de consola)`
5. `Help (Ayuda)`
6. `Exit (Salir)`

NOTA: Aunque puede haber varias sesiones de SOL activas al mismo tiempo, sólo puede haber una sesión de redirección de consola activa en un momento dado para un sistema administrado.

NOTA: Para salir de una sesión de SOL activa, utilice la secuencia de caracteres <~><.>. Esta secuencia finaliza SOL y le devuelve al menú de nivel superior.

1. Seleccione la opción 1 en el menú principal.

2. Introduzca la **dirección IP del iDRAC** del sistema administrado remoto.

3. Proporcione el **Nombre de usuario** y la **Contraseña** para iDRAC6 en el sistema administrado. El nombre de usuario y la contraseña del iDRAC6 se deben asignar y almacenar en el almacenamiento no volátil del iDRAC6.

   NOTA: Sólo se permite una sesión de redirección de consola SOL con iDRAC6 a la vez.

   NOTA: De ser necesario, extienda la duración de la sesión SOL a un número infinito de la siguiente manera: cambie el valor de **Límite de tiempo de Telnet** a cero en la interfaz gráfica web del usuario del iDRAC6, en **Sistema** → **Acceso remoto** → **iDRAC** → **Red / Seguridad** → **Servicios**.

4. Proporcione la clave de cifrado de IPMI si ésta se configuró en el iDRAC.

   NOTA: Puede encontrar la clave de cifrado de IPMI en la interfaz gráfica para el usuario del iDRAC6 en **Sistema** → **Acceso remoto** → **iDRAC** → **Red / Seguridad** → **Red** → **Configuración de la LAN IPMI** → **Clave de cifrado**.

   NOTA: La clave predeterminada sólo contiene ceros. Si presiona <Entrar> para la opción de cifrado, el iDRAC6 utilizará esta clave de cifrado predeterminada.

5. Seleccione **Configurar la comunicación en serie en la LAN para el servidor remoto** (opción 2) en el menú principal.

   Aparecerá el menú de configuración de SOL. De acuerdo con el estado de SOL actual, el contenido del menú de configuración de SOL varía:

   - Si SOL ya está activado, los valores actuales se muestran y se presentan tres posibilidades:

     1. `Disable Serial-Over-LAN (Desactivar Serial-Over-LAN)`
     2. `Change Serial-Over-LAN settings (Cambiar la configuración de la comunicación en serie en la LAN)`
     3. `Cancel (Cancelar)`

   - Si SOL está activada, asegúrese de que la velocidad en baudios de SOL coincida con la del iDRAC y que se requiera un mínimo nivel de privilegios de **administrador** del iDRAC6 para activar la redirección de consola.
   - Si SOL está desactivada, escriba `Y` para activar esta función o bien `N` para mantenerla en ese estado.

- Seleccione **Activar la redirección de consola** (opción 3) en el menú principal

  La consola de texto del sistema administrado remoto se redirige a la estación de administración.

7. Seleccione **Reiniciar y activar redirección de consola** (opción 4) en el menú principal (opcional).

   Se confirmará el estado de alimentación del sistema administrado remoto. Si la alimentación está activada, se le pedirá que decida entre un apagado ordenado o forzado.

   Después, el estado de alimentación es supervisado hasta que el estado cambie a **encendido**. La redirección de consola comienza y la consola de texto del sistema administrado remoto se redirige a la estación de administración.

   Mientras el sistema administrado se reinicia, puede acceder al programa de configuración del sistema del BIOS para ver o configurar los valores del BIOS.

8. Seleccione **Ayuda** (opción 5) en el menú principal para visualizar descripciones detalladas de cada opción.

9. Seleccione **Salir** (opción 6) en el menú principal para finalizar la sesión de Telnet y desconectarse del proxy SOL.

NOTA: Si un usuario no finaliza la sesión correctamente, ejecute el siguiente comando para reiniciar el iDRAC. Espere entre 1 y 2 minutos hasta que el iDRAC6 se inicie por completo. Consulte "Generalidades del subcomando RACADM" para obtener más información.

```
racadm racreset
```

Configuración del sistema operativo

Complete los siguientes pasos para configurar sistemas operativos genéricos de tipo Unix. Esta configuración toma como base las instalaciones predeterminadas de Red Hat Enterprise Linux 5.0, SUSE Linux Enterprise Server 10 SP1 y Windows 2003 Enterprise.

Sistema operativo Linux Enterprise

1. Edite el archivo **/etc/inittab** para activar el control de flujo de hardware y permitir que los usuarios inicien sesión a través de la consola SOL. Agregue la siguiente línea al final de la sección `#Ejecutar gettys en los niveles de ejecución estándares.`

```
7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
```

Ejemplo original de /etc/inittab:

```
_____________________________________________________________________

#

# inittab This file describes how the INIT process should set up

# the system in a certain run-level. (Este archivo

# describe la manera en la que el proceso INIT deberá

# configurar el sistema en un nivel de ejecución determinado.

#


SKIP this part of file


# Run gettys in standard runlevels (Ejecutar gettys en los niveles de ejecución estándares)

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1


# Run xdm in runlevel 5 (Ejecutar xdm en el nivel de ejecución 5)

x:5:respawn:/etc/X11/prefdm -nodaemon

_____________________________________________________________________
```

Ejemplo modificado de /etc/inittab:

```
_____________________________________________________________________

#

#

# inittab This file describes how the INIT process should set up

# the system in a certain run-level. (Este archivo

# describe la manera en la que el proceso INIT deberá
```

```
# configurar el sistema en un nivel de ejecución determinado.

#

SKIP this part of file

# Run gettys in standard runlevels (Ejecutar gettys en los niveles de ejecución estándares)

1:2345:respawn:/sbin/migetty tty1

2:2345:respawn:/sbin/migetty tty1

3:2345:respawn:/sbin/migetty tty1

4:2345:respawn:/sbin/migetty tty1

5:2345:respawn:/sbin/migetty tty1

6:2345:respawn:/sbin/migetty tty1

7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# Run xdm in runlevel 5 (Ejecutar xdm en el nivel de ejecución 5)

x:5:respawn:/etc/X11/prefdm -nodaemon
```

---

2. Edite el archivo **/etc/securetty** para permitir que los usuarios inicien sesión como root a través de la consola SOL. Agregue la siguiente línea después de consola:

   ```
   ttyS0
   ```

Ejemplo original de /etc/securetty:

```
consola

vc/1

vc/2

vc/3

vc/4

SKIP the rest of file
```

Ejemplo modificado de /etc/securetty:

```
Consola

ttyS0

vc/1

vc/2

vc/3

vc/4

SKIP the rest of file
```

---

3. Edite el archivo **/boot/grub/grub.conf** o el archivo **/boot/grub/menu.list** para agregar opciones de inicio para SOL:
   a. Agregue comentarios para las líneas de gráficos en los sistemas operativos de tipo Unix:
      - `splashimage=(had0,0)/grub/splash.xpm.gz` en RHEL 5
      - `gfxmenu (hda0,5)/boot/message` en SLES 10

b. Agregue la siguiente línea antes de la primera línea `title= ...`:

```
# Redirect OS boot via SOL (Redirigir inicio de sistema operativo a través de SOL)
```

c. Añada la siguiente entrada a la primera línea `title= ...`:

```
Redirección SOL
```

d. Agregue el siguiente texto a la línea `kernel/...` del primer `title= ...`:

```
consola=tty1 consola=ttyS0,115200
```

NOTA: **/boot/grub/grub.conf** en Red Hat Enterprise Linux 5 es un vínculo simbólico con **/boot/grub/menu.list**. Puede cambiar la configuración en uno de los dos.

Ejemplo original de /boot/grub/grub.conf en RHEL 5:

```
# grub.conf # grub.conf generated by anaconda (generado por anaconda)
#
# Note that you do not have to return grub after making changes to this
# file
# (Tenga en cuenta que no tiene que volver a ejecutar grub
# después de hacer cambios en este archivo)
# NOTICE: You have a /boot partition. This means that
# all kernel and initrd paths are relative to /boot/, eg.
# (AVISO: Tiene una partición /boot. Esto significa que
# todas las rutas de acceso initrd y kernel son relativas a /boot/, por ej.
# root (hd0,0)
# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00
# initrd /initrd-version.img
#boot=/dev/sda
valor predeterminado=0
tiempo de espera=5
splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

título Red Hat Enterprise Linux 5
     root (hd0,0)
     kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet
     initrd /initrd-2.6.18-8.el5.img
```

Ejemplo modificado de /boot/grub/grub.conf:

```
# grub.conf # grub.conf generated by anaconda (generado por anaconda)
#
# Note that you do not have to return grub after making changes to this
# file
# (Tenga en cuenta que no tiene que volver a ejecutar grub
# después de hacer cambios en este archivo)
# NOTICE: You have a /boot partition. This means that
```

```
# all kernel and initrd paths are relative to /boot/, eg.
# (AVISO: Tiene una partición /boot. Esto significa que
# todas las rutas de acceso initrd y kernel son relativas a /boot/, por ej.
# root (hd0,0)
# kernel /vmlinux-version ro root=/dev/VolGroup00/LogVol00
# initrd /initrd-version.img
#boot=/dev/sda
valor predeterminado=0
tiempo de espera=5
#splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

# Redirect the OS boot via SOL (Redirigir inicio de sistema operativo a través de SOL)
título Red Hat Enterprise Linux 5 redirección SOL
     root (hd0,0)
     kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00 rhgb quiet consola=tty1 consola=ttyS0,115200
     initrd /initrd-2.6.18-8.el5.img
```

Ejemplo original de /boot/grub/menu.list en SLES 10:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09
# (Modificado por YaST2. Última modificación: Sáb 11 oct 21:52:09 UTC 2008)
UTC 2008
Default 0
Timeout 8
gfxmenu (hd0.5)/boot/message
###Don't change this comment - YaST2 identifier: Original name: linux (No cambie este comentario. Identificador YaST2: Nombre original:
linux )###
title SUSE Linux Enterprise Server 10 SP1
     root (hd0,5)
     kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts
     initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Ejemplo modificado de /boot/grub/menu.list en SLES 10:

```
#Modified by YaST2. Last modification on Sat Oct 11 21:52:09
#(Modificado por YaST2. Última modificación: Sáb 11 oct 21:52:09)
UTC 2008
Default 0
Timeout 8
#gfxmenu (hd0.5)/boot/message

###Don't change this comment - YaST2 identifier: Original name: linux (No cambie este comentario. Identificador YaST2: Nombre original:
linux )###
```

título SUSE Linux Enterprise Server 10 SP1 **redirección SOL**

```
root (hd0,5)

kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts
consola=tty1 consola=ttyS0,115200

initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Windows 2003 Enterprise

1. Determine la identificación de entrada de inicio de la siguiente manera: ingrese bootcfg en la ventana del indicador de comandos de Windows. Localice la identificación de entrada de inicio de la sección con el nombre de sistema operativo **Windows Server 2003 Enterprise**. Presione <Entrar> para ver las opciones de inicialización en la estación de administración.

2. Active EMS en una ventana de petición de comandos de Windows ingresando el siguiente comando:

   ```
   bootcfg /EMS ON /PORT COM1 /BAUD 115200 /ID <Id. de inicialización>
   ```

   NOTA: <*Id. de inicialización*> será la identificación de entrada de inicio del paso 1.

3. Presione <Entrar> para verificar que la configuración de la consola EMS surta efecto.

Ejemplo de configuración original de bootcfg:

```
Boot Loader Settings

--------------------

timeout:30

default:multi(0)disk(0)rdisk(0)partition(1)\WINDOWS


Boot Entries

------------

Boot entry ID: 1

Os Friendly Name: Winodws Server 2003, Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

Ejemplo modificado de configuración bootcfg:

```
Boot Loader Settings

--------------------

timeout: 30

default: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

redirect: COM1

redirectbaudrate:115200


Boot Entries

------------

Boot entry ID: 1

Os Friendly Name: Windows Server 2003, Enterprise

Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
```

```
     OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect
```

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la redirección de consola con interfaz gráfica de usuario

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Esta sección proporciona información acerca de cómo usar la función de redirección de consola del iDRAC6.

Información general

La función consola de redirección del iDRAC6 le permite acceder en forma remota a consolas locales en modos de gráficos o de texto; así, puede controlar uno o varios sistemas equipados con iDRAC6 desde una única ubicación.

Uso de redirección de consola

NOTA: Cuando usted abre una sesión de redirección de consola, el servidor administrado no indica que la consola ha sido redirigida.

La pantalla **Redirección de consola** permite administrar el sistema remoto con el teclado, vídeo y ratón en su estación de administración local para controlar los dispositivos correspondientes en un servidor administrado remoto. Esta característica puede ser usada junto con la característica de medios virtuales para realizar instalaciones de software remotas.

Las reglas siguientes se aplican a una sesión de redirección de consola:

- Sólo se admite un máximo de dos sesiones simultáneas de redirección de consola. Ambas sesiones muestran la misma consola de servidor administrado simultáneamente.
- La sesión de redirección de consola no se deberá ejecutar desde un explorador web en el sistema administrado.
- Se requiere un ancho de banda disponible de red de 1 MB/s.

Si un segundo usuario solicita una sesión de redirección de consola, el primer usuario recibe una notificación y se brinda la opción de rechazar el acceso, permitir sólo vídeo o permitir el acceso compartido completo. El segundo usuario es notificado que otro usuario tiene el control. El primer usuario debe responder en treinta segundos o se otorgará automáticamente el acceso completo al segundo usuario. Cuando hay dos sesiones activas de forma simultánea, cada usuario ve un mensaje en la esquina superior derecha de la pantalla que identifica al otro usuario que tiene una sesión activa. No se permite una tercera sección activa. Si un tercer usuario solicita una sesión de redirección de consola, se le deniega el acceso sin interrumpir las sesiones del primer o segundo usuario.

Si ni el primer ni el segundo usuario tienen privilegios de administrador, la finalización de la sección activa del primer usuario finaliza también la sesión del segundo usuario.

Resoluciones de pantalla y velocidades de actualización admitidas

La tabla 10-1 muestra una lista de las resoluciones admitidas de pantalla y las velocidades de actualización correspondientes para una sesión de redirección de consola que se ejecuta en el servidor administrado.

Tabla 10-1. Resoluciones de pantalla y velocidades de actualización admitidas

Resolución de pantalla	Velocidad de actualización (Hz)
720 x 400	70
640 x 480	60, 72, 75, 85
800 x 600	60, 70, 72, 75, 85
1024 x 768	60, 70, 72, 75, 85
1280 x 1024	60

Configuración de la estación de administración

Para usar la Redirección de consola en la estación de administración, realice el siguiente procedimiento:

1. Instale y configure un explorador de web admitido. Consulte "Exploradores web admitidos" y "Configuración de un explorador de web admitido".
2. Si usa Firefox o desea usar el visor de Java con Internet Explorer, instale Java Runtime Environment (JRE). Consulte "Instalación de Java Runtime

Environment (JRE)".

3. Dell recomienda que configure la resolución de su monitor en 1280 x 1024 pixeles.

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, se cambiará de Linux a consola de texto.

Configuración de la redirección de consola y Medios virtuales en la interfaz web del iDRAC6

Para configurar la redirección de consola en la interfaz web del iDRAC6, realice los pasos a continuación:

1. Haga clic en **Sistema** y después haga clic en la ficha **Consola**.
2. Haga clic en **Configuración** para abrir la pantalla **Configuración de la redirección de consola**.
3. Configure las propiedades de la redirección de consola. La tabla 10-2 describe la configuración de la redirección de consola.
4. Cuando termine, haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente. Vea la tabla 10-3.

Tabla 10-2. Propiedades de configuración de la redirección de consola

Propiedad	Descripción
Activado	Haga clic para activar o desactivar la Redirección de consola. **Seleccionado** indica que la redirección de consola está activada. **Deseleccionado** indica que la redirección de consola está desactivada. El valor predeterminado es **activado**.
N° máx. de sesiones	Muestra el número máximo posible de sesiones de redirección de consola, **1** ó **2**. Use el menú desplegable para cambiar el número máximo posible de sesiones de Redirección de consola. El valor predeterminado es **2**.
Sesiones activas	Muestra el número de sesiones de Consola activa. Este campo es de sólo lectura.
Número del puerto de teclado y mouse	El número de puerto de red utilizado para conectar a la opción de teclado/mouse de la Redirección de consola. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es **5900**.
Número del puerto de vídeo	El número de puerto de red utilizado para conectar a la opción de teclado/mouse de la Redirección de consola. Se recomienda cambiar este valor si otro programa está usando el puerto predeterminado. El valor predeterminado es **5901**.
Cifrado de vídeo activado	**Seleccionado** indica que el cifrado de vídeo está activado. Todo el tráfico que se dirige al puerto de vídeo está cifrado. **Deseleccionado** indica que el cifrado de vídeo está desactivado. El tráfico que va al puerto de vídeo no está cifrado. El valor predeterminado es **Cifrado. La desactivación del cifrado puede mejorar el rendimiento en las redes más lentas.**
Modo Mouse	Elija **Windows** cuando el servidor administrado se esté ejecutando en un sistema operativo Windows. Elija **Linux** si el servidor ejecuta Linux. Elija **Sin acceso** si el servidor no está funcionando en un sistema operativo Windows o Linux. **NOTA:** Debe seleccionar **Modo ratón sin acceso** en HyperV, Dell Diagnostics o USC. El valor predeterminado es **Windows**.
Tipo de complemento de la consola para IE	Cuando use Internet Explorer en un sistema operativo Windows, puede elegir entre los siguientes visores: *ActiveX*: el visor *ActiveX para redirección de consola* Java: el visor *Java para Redirección de consola*. **NOTA:** Según su versión de Internet Explorer, deberá desactivar restricciones de seguridad adicionales (consulte "Configuración y uso de medios virtuales"). **NOTA:** Deberá tener instalado Java Runtime Environment en el sistema cliente a fin de usar el visor de Java.
Vídeo del servidor local activado	**Seleccionado** indica que la salida al monitor iKVM está activada durante la redirección de consola. **Deseleccionado** indica que las tareas que realice con **Redirección de consola** no se verán en el monitor local del servidor administrado.

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

Los botones en la tabla 10-5 están disponibles en la pantalla **Configuración de la redirección de consola**.

Tabla 10-3. Botones de configuración de redirección de consola

Botón	Definición
Imprimir	Imprime la pantalla **Configuración de la redirección de consola**
Actualizar	Vuelve a cargar la pantalla **Configuración de la redirección de consola**
Aplicar	Guarda todos los nuevos valores de configuración realizados en la redirección de consola.

Abrir una sesión de redirección de consola

Cuando abre una sesión de redirección de consola, la aplicación Dell Virtual KVM Viewer se inicia y aparece el escritorio del sistema remoto en el visor. Al usar la aplicación Virtual KVM Viewer, puede controlar las funciones de mouse y teclado del sistema remoto desde la estación de administración local.

Para abrir una sesión de redirección de consola en la interfaz web, realice los pasos a continuación:

1. Haga clic en **Sistema** y después haga clic en la ficha **Consola**.
2. En la pantalla **Redirección de consola**, utilice la información en la tabla 10-4 para verificar que haya una sesión de redirección de consola disponible.

   Si desea volver a configurar los valores de propiedades que se muestran, consulte "Configuración de la redirección de consola y Medios virtuales en la interfaz web del iDRAC6".

Tabla 10-4. Información sobre redirección de consola

Propiedad	Descripción
Redirección de consola activada	Sí/No
Cifrado de vídeo activado	Sí/No
N° máx. de sesiones	Muestra el número máximo de sesiones de redirección de consola admitidas.
Sesiones actuales	Muestra el número actual de sesiones de redirección de consola activas.
Modo Mouse	Muestra la aceleración actual del mouse. El modo de **Aceleración del mouse** se debe elegir con base en el tipo de sistema operativo instalado en el servidor administrado.
Tipo de complemento de consola	Muestra el tipo de complemento actualmente configurado. **ActiveX**: se iniciará un visor Active-X. El visor Active-X únicamente funciona en Internet Explorer cuando se ejecuta en un sistema operativo Windows. **Java**: se iniciará un visor Java. El visor Java se puede usar en cualquier explorador incluso Internet Explorer. Si el cliente se ejecuta en un sistema operativo que no sea Windows, entonces debe usar el visor Java. Si está accediendo al iDRAC6 desde Internet Explorer con un sistema operativo Windows, puede elegir el tipo de complemento, ya sea ActiveX o Java.
Vídeo del servidor local activado	Seleccionado indica que la salida al monitor iKVM está activada durante la redirección de consola. Deseleccionado garantiza que las tareas que realice mediante la **Redirección de consola** no se verán en el monitor local del servidor administrado.

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

Los botones en la tabla 10-5 están disponibles en la pantalla **Redirección de consola**.

Tabla 10-5. Botones de redirección de consola

Botón	Definición
Actualizar	Vuelve a cargar la pantalla **Configuración de la redirección de consola**
Iniciar el visor	Abre una sesión de redirección de consola en el sistema remoto de destino
Imprimir	Imprime la pantalla **Configuración de la redirección de consola**

3. Si hay una sesión de redirección de consola disponible, haga clic en **Iniciar el visor**.

   NOTA: Pueden aparecer varias ventanas de mensaje después de iniciar la aplicación. Para evitar el acceso no autorizado a la aplicación, navegue a través de estas ventanas de mensajes dentro de tres minutos. De lo contrario, se le pedirá iniciar la aplicación nuevamente.

   NOTA: Si una o varias ventanas de **Alerta de seguridad** aparecen en los pasos siguientes, lea la información en la ventana y haga clic en **Sí** para seguir.

La estación de administración se conecta al iDRAC6 y la pantalla de escritorio del sistema remoto aparece en la aplicación Dell Digital KVM Viewer.

4. Aparecerán dos apuntadores de mouse en la ventana del visor: uno para el sistema remoto y otro para el sistema local. Usted deberá sincronizar los dos apuntadores del mouse de manera que el apuntador del mouse remoto siga el apuntador del mouse local. Consulte "Sincronización de los apuntadores del mouse".

Uso de Video Viewer

Video Viewer proporciona una interfaz de usuario entre la estación de administración y el servidor administrado que le permite ver la pantalla de escritorio del servidor administrado y controlar las funciones de mouse y teclado desde la estación de administración. Cuando se conecta con el sistema remoto, Video Viewer se inicia en otra ventana.

Video Viewer proporciona varios ajustes de control, por ejemplo, modo de color, sincronización del mouse, instantáneas, macros de teclado y acceso a los medios virtuales. Haga clic en **Ayuda** para obtener más información sobre estas funciones.

Cuando usted inicia una sesión de redirección de consola y Video Viewer aparece, es posible que deba ajustar el modo de color y sincronizar los apuntadores de mouse.

La tabla 10-6 describe las opciones del menú que están disponibles en el visor.

Tabla 10-6. Selecciones de la barra de menú del visor

Elemento del menú	Elemento	Descripción
Vídeo	Pausa	Pausa la redirección de consola temporalmente.
	Reanudar	Reanuda la redirección de consola.
	Actualizar	Vuelve a trazar la imagen de la pantalla del visor.
	Capturar la pantalla actual	Captura la pantalla actual del sistema remoto en un archivo **.bmp** en Windows o en un archivo **.png** en Linux. Aparece un cuadro de diálogo que permite guardar el archivo en un lugar determinado.
	Pantalla completa	Para expandir el Video Viewer al modo de pantalla completa, seleccione **Pantalla completa** desde el menú **Vídeo**.
	Salir	Cuando haya terminado de usar la consola y haya cerrado la sesión (mediante el procedimiento de desconexión del sistema remoto), haga clic en **Salir** desde el menú **Vídeo** para cerrar la ventana del **Video Viewer**.
Teclado	Mantener presionada la tecla Alt derecha	Seleccione este elemento antes presionar las teclas que desea combinar con la tecla <Alt> derecha.
	Mantenga presionada la tecla Alt izquierda	Seleccione este elemento antes de presionar las teclas que desea combinar con la tecla <Alt> izquierda.
	Tecla Windows izquierda	Seleccione **Mantener presionado** antes de teclear los caracteres que desea combinar con la tecla Windows izquierda. Seleccione **Presionar y soltar** para enviar una pulsación de la tecla Windows izquierda.
	Tecla Windows derecha	Seleccione **Mantener presionado** antes de teclear los caracteres que desea combinar con la tecla Windows derecha. Seleccione **Presionar y soltar** para enviar una pulsación de la tecla Windows derecha.
	Macros	Cuando selecciona una macro o presiona la tecla aceleradora especificada para la macro, la acción se ejecuta en el sistema remoto. El Video Viewer ofrece las macros a continuación: • Ctrl-Alt-Supr • Alt-Tab • Alt-Esc • Ctrl-Esc • Alt-Espacio • Alt-Entrar • Alt-Guión • Alt-F4 • ImprPant • Alt-ImprPant • F1 • Pausa • Alt+m
	Paso a través de teclado	El modo de paso a través de teclado permite que todas las funciones del teclado en el cliente se redirijan al servidor.
Ratón	Sincronizar el cursor	Sincroniza el cursor de modo que el ratón del cliente se redirija al ratón del servidor.
	Ocultar cursor local	Sólo aparecerá el cursor de KVM. Dell recomienda esta configuración cuando se ejecuta USC en vKVM.
Opciones	Modo de color	Permite seleccionar la profundidad del color para mejorar el rendimiento en la red. Por ejemplo, si va a instalar software a partir de medios virtuales, puede seleccionar la profundidad en color más baja (gris de 3 bits), de manera que el visor de consola use menos ancho de banda y se destine mayor ancho de banda a la transferencia de datos de los medios. El modo de color se puede definir en color de 15 bits, color de 7 bits, color de 4 bits, gris de 4 bits y gris de 3 bits.
Medios	Asistente de medios virtuales	El menú **Medios** ofrece acceso al Asistente de medios virtuales, el cual permite redirigir a un dispositivo o imagen, por ejemplo: • Unidad de disco flexible • CD • DVD • Imagen en formato ISO • Unidad flash USB

		Para obtener información sobre la función de medios virtuales, consulte "Configuración y uso de medios virtuales". Se debe mantener activa la ventana del visor de consola cuando se usan los medios virtuales.
Ayuda	N/D	Activa el menú **Ayuda**.

Sincronización de los apuntadores del mouse

Cuando se conecta a un sistema PowerEdge remoto usando la redirección de consola, la velocidad de aceleración del mouse en el sistema remoto podría no sincronizarse con el apuntador del mouse en la estación de administración, ocasionando que aparezcan dos apuntadores de mouse en la ventana de Video Viewer.

Para sincronizar los apuntadores de mouse, haga clic en **Mouse**→ **Sincronizar el cursor** o presione <Alt><M>.

La opción del menú Sincronizar el cursor es un interruptor. Asegúrese que haya una marca a un lado de la opción del menú; esto indica que la sincronización del mouse está activada.

Cuando se usa Red Hat Enterprise Linux o Novell SUSE Linux, asegúrese de configurar el modo de ratón para Linux antes de iniciar el visor. Consulte "Configuración de la redirección de consola y Medios virtuales en la interfaz web del iDRAC6" para obtener ayuda con la configuración. La configuración predeterminada del ratón del sistema operativo se usa para controlar la flecha del ratón en la pantalla de **Redirección de consola** del iDRAC6.

Desactivación o activación de la consola local

Usted puede configurar el iDRAC6 para rechazar conexiones de iKVM por medio de la interfaz web del iDRAC6. Cuando la consola local está desactivada, aparece un punto amarillo de estado en la lista de servidores (OSCAR) para indicar que la consola está bloqueada en el iDRAC6. Cuando la consola local está activada, el punto de estado es verde.

Si desea asegurarse de tener acceso exclusivo a la consola del servidor administrado, deberá desactivar la consola local *y volver a configurar el* **Número máximo de sesiones** a 1 en la **pantalla de Redirección de consola**.

NOTA: La función de consola local es compatible con todos los sistemas PowerEdge x9xx, excepto los PowerEdge SC1435 y 6950.

NOTA: Si desactiva (apaga) el vídeo local en el servidor, se desactivarán el monitor, teclado y mouse que están conectados al iKVM.

Para desactivar o activar la consola local, realice el procedimiento siguiente:

1. En la estación de administración, abra un explorador web admitido e inicie sesión en el iDRAC6. Consulte "Acceso a la interfaz web" para obtener más información.
2. Haga clic en **Sistema**, haga clic en la ficha **Consola** y después haga clic en **Configuración**.
3. Si desea desactivar (apagar) el vídeo local en el servidor, en la pantalla **Configuración de la redirección de consola**, deseleccione la casilla **Vídeo del servidor local activado** y después haga clic en **Aplicar.** El valor predeterminado es **Activado (seleccionado)**.
4. Si desea activar (encender) el vídeo local en el servidor, en la pantalla **Configuración de la redirección de consola**, seleccione la casilla **Vídeo del servidor local activado** y después haga clic en **Aplicar**.

La pantalla **Redirección de consola** muestra el estado del Vídeo del servidor local.

Preguntas frecuentes

La tabla 10-7 contiene las preguntas y respuestas frecuentes.

Tabla 10-7. Uso de la redirección de consola: preguntas frecuentes

Pregunta	Respuesta
¿Se puede iniciar una nueva sesión de vídeo de consola remota cuando el vídeo local del servidor está apagado?	Sí
¿Por qué tarda 15 segundos apagar el vídeo local del servidor después de solicitar la desactivación del vídeo local?	Esto brinda al usuario local la oportunidad de realizar alguna acción antes de que el vídeo se apague.
¿Hay algún retraso al encender el vídeo local?	No, una vez que el iDRAC6 recibe la solicitud de **encendido** del vídeo local, este último se enciende instantáneamente.
¿El usuario local también puede apagar el vídeo?	Sí, el usuario local puede usar la CLI de RACADM local para apagar el vídeo.
¿El usuario local también puede encender el vídeo?	No. Después de que la consola local se desactive, el teclado y el mouse del usuario local se desactivarán y no podrán hacer cambios de configuración.
¿La desactivación del vídeo local también desactiva el teclado y el	Sí

mouse locales?	
¿La desactivación de la consola local desactivará el vídeo en la sesión de consola remota?	No, la activación o desactivación del vídeo local es independiente de la sesión de consola remota.
¿Cuáles son los privilegios necesarios para que un usuario de iDRAC6 active o desactive el vídeo del servidor local?	Cualquier usuario con privilegios de configuración del iDRAC6 puede activar o desactivar la consola local.
¿Cómo se puede ver el estado actual del vídeo del servidor local?	El estado se muestra en la pantalla **Configuración de la redirección de consola** de la interfaz web del iDRAC6. El comando **racadm getconfig -g cfgRacTuning** de la CLI de RACADM muestra el estado en el objeto **cfgRacTuneLocalServerVideo**. El estado también se muestra en la pantalla de OSCAR de iKVM. Cuando la consola local está activada, aparece un indicador de estado verde al lado del nombre del servidor. Cuando está desactivada, un punto amarillo indica que el iDRAC6 ha bloqueado la consola local.
No puedo ver la parte inferior de la pantalla del sistema en la ventana de redirección de consola.	Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024.
La ventana de la consola no es legible.	El visor de la consola en Linux requiere de un conjunto de caracteres UTF-8. Revise la configuración regional y, de ser necesario, restablezca el conjunto de caracteres. Para obtener más información, consulte "Cómo establecer la configuración regional en Linux".
¿Por qué aparece una pantalla en blanco en el servidor administrado al cargar el sistema operativo Windows 2000?	El servidor administrado no tiene el archivo controlador correcto de vídeo ATI. Deberá actualizar el controlador de vídeo con el CD *Dell PowerEdge Installation and Server Management*.
¿Por qué el mouse no se sincroniza en DOS cuando se ejecuta la redirección de consola?	El BIOS de Dell emula el controlador de mouse como mouse PS/2. Debido al diseño, el mouse PS/2 usa la posición relativa para el apuntador de mouse, lo que ocasiona un retraso en la sincronización. El iDRAC6 tiene un controlador de ratón USB, que permite la posición absoluta y un seguimiento más preciso del apuntador del ratón. Aun cuando el iDRAC6 pasara la posición absoluta del ratón USB al BIOS de Dell, la emulación del BIOS lo convertiría nuevamente a la posición relativa y el comportamiento seguiría siendo el mismo. Para resolver este problema, defina el modo de ratón como **Sin acceso** en la configuración de Redirección de consola.
¿Por qué no se sincroniza el mouse en la consola de texto de Linux?	El KVM virtual necesita el controlador de mouse USB, pero el controlador de mouse USB sólo está disponible en el sistema operativo X-Window.
Aún tengo problemas con la sincronización del mouse.	Compruebe que el mouse adecuado esté seleccionado para el sistema operativo antes de iniciar una sesión de redirección de consola. Compruebe que **Sincronizar el mouse** esté seleccionado en el menú **Mouse**. Presione <Alt><M> o seleccione **Mouse→ Sincronizar el mouse** para activar/desactivar la sincronización del mouse. Cuando la sincronización esté activada, aparecerá una marca junto a la selección en el menú **Mouse**.
¿Por qué no puedo usar un teclado o ratón mientras instalo un sistema operativo de Microsoft® de manera remota por medio de la redirección de consola del iDRAC6?	Cuando instala de manera remota un sistema operativo Microsoft admitido en un sistema con la redirección de consola habilitada en el BIOS, aparece un mensaje de conexión de EMS que le pide que seleccione **Aceptar** para poder continuar. Usted no puede usar el mouse para seleccionar **Aceptar** de manera remota. Debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, volver a instalar y luego desactivar la redirección de consola en el BIOS. Microsoft genera este mensaje para avisar al usuario que la redirección de consola está activada. Para asegurar que este mensaje no aparece, siempre desactive la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota.
¿Por qué el indicador de Bloq Núm de mi estación de administración no muestra el estado de Bloq Núm en el servidor remoto?	Cuando se accede por medio del iDRAC6, el indicador Bloq Num de la estación de administración no necesariamente coincide con el estado del Bloq Num del servidor remoto. El estado de Bloq Núm depende de la configuración en el servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Núm en la estación de administración.
¿Por qué aparecen varias ventanas de Session Viewer cuándo establezco una sesión de redirección de consola desde el host local?	Usted está configurando una sesión de redirección de consola desde el sistema local. Esto no se permite.
Si ejecuto una sesión de redirección de consola y un usuario local accede al servidor administrado ¿recibiré un mensaje de advertencia?	No. Si un usuario local tiene acceso al sistema, tendrán el control del sistema.
¿Cuánto ancho de banda necesito para ejecutar una sesión de redirección de consola?	Dell recomienda una conexión de 5 MB/s para un buen rendimiento. Se requiere una conexión de 1 MB/s para un rendimiento mínimo.
¿Cuáles son los requisitos mínimos del sistema para que mi estación de administración ejecute la redirección de consola?	Se requiere que la estación de administración tenga un procesador Intel Pentium III a 500 MHz con al menos 256 MB de RAM.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de una tarjeta multimedia VFlash para utilizar con iDRAC6

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

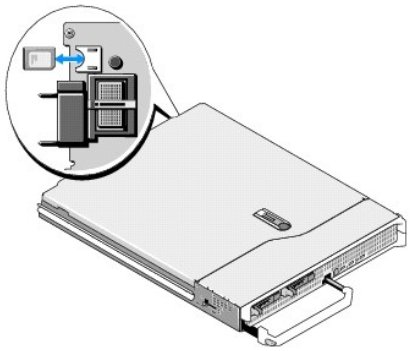
La tarjeta multimedia VFlash es una tarjeta Secure Digital (SD) que se conecta en la ranura para tarjeta opcional del iDRAC6 Enterprise ubicada en la esquina posterior del sistema. Proporciona espacio de almacenamiento que actúa como un dispositivo USB Flash común.

Instalación de una tarjeta multimedia VFlash

NOTA: Se necesita una tarjeta multimedia vFlash marca Dell para la partición flash virtual.

1. Extraiga el módulo de alta densidad del chasis.
2. Localice la ranura para tarjetas multimedia VFlash en la esquina posterior del sistema.

   NOTA: No es necesario extraer la cubierta del módulo de alta densidad para instalar o extraer la tarjeta.



3. Con la cara de la etiqueta hacia arriba, inserte en la ranura para tarjeta del módulo la tarjeta SD por el extremo con los contactos.

   NOTA: La ranura está diseñada para que la tarjeta se inserte correctamente.

4. Presione hacia dentro la tarjeta para bloquearla en la ranura.
5. Vuelva a colocar el módulo de alta densidad en el chasis.

Extracción de una tarjeta multimedia VFlash

Para extraer la tarjeta multimedia VFlash, presione hacia adentro en la tarjeta para liberarla y sáquela de la ranura para tarjeta.

Configuración de la tarjeta multimedia VFlash con la interfaz web del iDRAC6

Activar o desactivar la tarjeta multimedia VFlash

NOTA: La casilla **VFlash Activada** está activa sólo si se ha insertado una tarjeta VFlash. Si no insertó una tarjeta, aparece el siguiente mensaje:

```
SD Card not inserted. Please insert an SD card of size greater than 256MB.
(Tarjeta SD no insertada. Inserte una tarjeta SD de tamaño mayor a 256MB.)
```

1. Asegúrese de que la tarjeta VFlash esté instalada.

2. Abra una ventana de un explorador web compatible.
3. Inicie sesión en la interfaz Web del iDRAC6.
4. Seleccione **Sistema** en el árbol del sistema.
5. Haga clic en la ficha **VFlash**.

   Aparece la pantalla **VFlash**.
6. Seleccione la casilla **Activar VFlash** para activar la tarjeta multimedia VFlash. Para desactivarla, deseleccione la casilla.
7. Haga clic en **Aplicar**.

Formatear la tarjeta multimedia VFlash

NOTA: La opción **Formatear** está activa sólo si se ha insertado una tarjeta VFlash.

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Seleccione **Sistema** en el árbol del sistema.
3. Haga clic en la ficha **VFlash**.

   Aparece la pantalla **VFlash**.
4. Asegúrese que VFlash esté desactivada. La casilla **VFlash activada** debe estar vacía (sin seleccionar).
5. Haga clic en **Formatear**.

   Aparecerá una casilla de alerta, con la advertencia de que se borrará toda imagen que esté en la tarjeta durante el proceso y solicitará confirmación. Haga clic en **Aceptar** para continuar.

   Aparecerá una barra de estado que indicará la evolución del proceso de formato.

Cargar imagen de disco

1. Asegúrese de que el archivo de imagen tenga una extensión .img y que la imagen no tenga un tamaño mayor que 256 MB.

   NOTA: Si bien su tarjeta VFlash puede ser de tamaño mayor que 256 MB, sólo se puede acceder a 256 MB en este momento.
2. Inicie sesión en la interfaz Web del iDRAC6.
3. Seleccione **Sistema** en el árbol del sistema.
4. Haga clic en la ficha **VFlash**.

   Aparece la pantalla **VFlash**.
5. Asegúrese que VFlash esté desactivada. La casilla **VFlash activada** debe estar vacía (sin seleccionar).
6. En la sección **Unidad VFlash**, ingrese la ruta de acceso al archivo de imagen o haga clic en **Examinar** para ubicarla en el sistema.

   Haga clic en **Cargar**.

   Aparecerá una barra de estado que indicará la evolución del proceso de carga.

Visualización del tamaño de la tarjeta VFlash

El menú desplegable **Tamaño de la memoria flash virtual** muestra la configuración de tamaño actual.

Configuración de la tarjeta multimedia VFlash con RACADM

Activar o desactivar la tarjeta multimedia VFlash

Abra una consola local al servidor, inicie sesión y escriba:

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 ó 0 ]
```

en donde `1` significa activada y `0` significa desactivada.

NOTA: Para obtener más información acerca de cfgRacVirtual, incluso los detalles de mensajes de salida, consulte cfgRacVirtual.

Formatear la tarjeta multimedia VFlash

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

```
racadm vmkey reset
```

PRECAUCIÓN: Al formatear la tarjeta multimedia VFlash, se eliminará toda la información existente.

NOTA: Para obtener más información acerca de vmkey, consulte "vmkey".

Regresar a la página de contenido

Regresar a la página de contenido

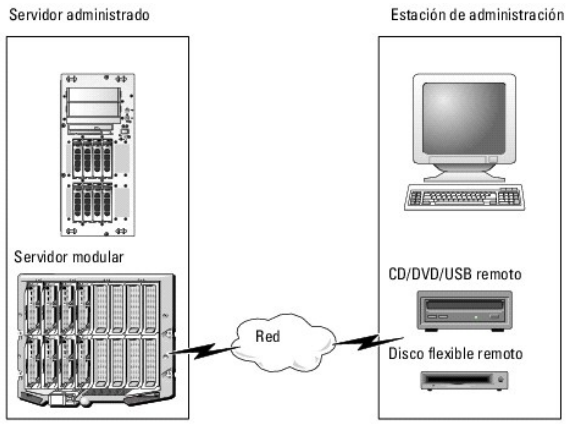
Configuración y uso de medios virtuales

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Información general

El componente **Medios virtuales**, que puede encontrar a través del visor de redirección de consola, permite que el servidor administrado tenga acceso a medios conectados a un sistema remoto en la red. La figura 12-1 muestra la arquitectura general de los **Medios virtuales**.

Figura 12-1. Arquitectura general de medios virtuales



Por medio de los **Medios virtuales**, los administradores pueden iniciar los servidores administrados, instalar aplicaciones, actualizar archivos controladores o incluso instalar nuevos sistemas operativos de manera remota desde las unidades de CD/DVD y de disco virtuales.

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

Los **Medios virtuales** definen dos dispositivos para el sistema operativo y el BIOS del servidor administrado: un dispositivo de disco flexible y un dispositivo de disco óptico.

La estación de administración proporciona los medios físicos o el archivo de imagen a través de la red. Cuando los **Medios virtuales** se conectan, todas las solicitudes de acceso a la unidad virtual de CD o de disco flexible provenientes del servidor administrado son dirigidas a la estación de administración por la red. La conexión de los **Medios virtuales** tiene el mismo efecto que insertar discos en los dispositivos físicos. Cuando los medios virtuales no están conectados, los dispositivos virtuales en el servidor administrado se comportan como dos unidades sin discos insertados en ellas.

La tabla 12-1 lista las conexiones compatibles de unidades ópticas virtuales y de disco flexible virtuales.

NOTA: Si cambia los **medios virtuales** mientras están conectados se podría detener la secuencia de inicio de sistema.

Tabla 12-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disco flexible virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disco flexible heredada de 1,44 pulgadas con disquete de 1,44 pulgadas	Unidad combinada de CD-ROM, DVD, CD-RW, con disco CD-ROM
Unidad de disco flexible USB con un disquete de 1,44 pulgadas	Archivo de imagen de CD-ROM/DVD en el formato ISO9660
Imagen de disco flexible de 1,44 pulgadas	Unidad USB de CD-ROM con disco CD-ROM
Disco USB extraíble (tamaño mínimo de 128 MB)	

Estación de administración con Windows

Para ejecutar la función de **Medios virtuales** en una estación de administración que ejecuta el sistema operativo Windows, instale una versión compatible de

Internet Explorer con el complemento de control de ActiveX (consulte "Exploradores web admitidos"). Establezca la seguridad del explorador en el nivel **Medio** o en un nivel inferior para permitir que Internet Explorer descargue e instale los controles ActiveX firmados.

Dependiendo de su versión de Internet Explorer, es posible que se le solicite una configuración de seguridad personalizada para ActiveX:

1. Inicie el Internet Explorer.
2. Haga clic en **Herramientas**→ **Opciones de Internet** y después haga clic sobre la ficha **Seguridad**.
3. En **Seleccionar una zona de contenido web para especificar su configuración de seguridad**, haga clic para seleccionar la zona deseada.
4. En **Nivel de seguridad para esta zona,** haga clic en **Nivel personalizado**.

   Aparece la ventana **Configuración de seguridad.**
5. En **Controles y plug-ins ActiveX**, asegúrese de que las siguientes opciones estén fijadas en **Permitir**:
   - Permitir Scriptlets
   - Solicitud automática para controles de ActiveX
   - Descargar controles firmados de ActiveX
   - Descargar controles no firmados de ActiveX
6. Haga clic sobre **Aceptar** para guardar cualquier cambio y cierre la ventana de **Configuración de seguridad**.
7. Haga clic en **Aceptar** para cerrar la ventana de **Opciones de Internet Options**.
8. Reinicie Internet Explorer.

Se deben tener derechos de administrador para instalar ActiveX. Antes de instalar el control ActiveX, es posible que Internet Explorer muestre una advertencia de seguridad. Para completar el procedimiento de instalación del control ActiveX, acepte el control ActiveX cuando Internet Explorer muestre la advertencia de seguridad.

Estación de administración con Linux

Para ejecutar el componente de medios virtuales en una estación de administración que ejecuta el sistema operativo Linux, instale una versión admitida de Firefox. Consulte "Exploradores web admitidos" para obtener más información.

Se requiere Java Runtime Environment (JRE) para ejecutar el complemento de redirección de consola. Puede descargar JRE desde el sitio **java.sun.com**. Se recomienda la versión 1.6 o superiores de JRE.

Configuración de los medios virtuales

1. Inicie sesión en la interfaz Web del iDRAC6.
2. Haga clic en la ficha **Consola / Medios**.
3. Haga clic en **Configuración y luego en Medios virtuales**.

   Aparecerá la pantalla **Configuración de redirección de consola**.
4. Haga clic en **Medios virtuales**.
5. En la sección **Medios virtuales,** seleccione los valores para la configuración. Consulte la tabla 12-2 para obtener información sobre los valores de configuración de los **Medios virtuales**.
6. Haga clic en **Aplicar** para guardar la configuración.

   Aparecerá un cuadro de diálogo de alerta con el siguiente mensaje: `You are about to change device configuration. All existing redirection sessions will be closed. Do you want to continue? (Está a punto de cambiar la configuración del dispositivo. Se cerrarán todas las sesiones de redirección existentes. ¿Desea continuar?)`
7. Haga clic en **Aceptar** para continuar.

   Aparecerá un cuadro de diálogo de alerta con el siguiente mensaje: `Virtual Media Configuration successfully set. (La configuración de los medios virtuales se definió correctamente.)`

Tabla 12-2. Valores de configuración de los medios virtuales

Atributo	Valor
Conectar medios virtuales	**Conectar**: conecta inmediatamente los **Medios virtuales** al servidor. **Desconectar**: desconecta inmediatamente los **Medios virtuales** del servidor. **Conectar automáticamente**: conecta los **Medios virtuales** al servidor únicamente cuando se inicia una sesión de medios virtuales.
Número máximo de sesiones	Muestra el número máximo de sesiones de **Medios virtuales** permitidas. Este valor siempre es **1**. **NOTA:** Sólo se permite una única sesión de medios virtuales. Sin embargo, en una única sesión se pueden conectar múltiples dispositivos. Consulte "Ejecución de los medios virtuales".
Sesiones activas	Muestra el número actual de sesiones de medios virtuales.
Cifrado activado para medios virtuales	Activa (seleccionada) o desactiva (deseleccionada) el cifrado de las conexiones de **Medios virtuales**.
Número de puerto de los medios virtuales	El número de puerto de red que se usa para conectarse al servicio de **Medios virtuales** sin cifrado. Dos puertos consecutivos a partir del número de puerto especificado se usan para conectar al servicio de **Medios virtuales**. El número de puerto después del puerto especificado no se debe configurar para ningún otro servicio del iDRAC6. El valor predeterminado es **3668**.
Número de puerto SSL de los medios virtuales	El número de puerto de red utilizado para conexiones cifradas del servicio de **Medios virtuales**. Dos puertos consecutivos a partir del número de puerto especificado se usan para conectar al servicio de **Medios virtuales**. El número de puerto después del puerto especificado no se debe configurar para ningún otro servicio del iDRAC6. El valor predeterminado es **3670**.
Emulación de disco flexible	Indica si los **Medios virtuales** aparecen como unidad de disco flexible o como memoria USB en el servidor. Si se selecciona **Emulación de disco flexible**, el dispositivo **Medios virtuales** aparecerá como dispositivo de disco flexible en el servidor. Cuando se deselecciona, aparece como unidad de memoria USB.
Activar el inicio una vez	Activa (seleccionada) o desactiva (deseleccionada) la opción de inicio único, que cierra automáticamente la sesión de los **Medios virtuales** después de que el servidor se haya iniciado una vez. Esta opción es útil para implementaciones automáticas.

Ejecución de los medios virtuales

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

NOTA: La aplicación Visor de consola debe permanecer activa mientras usted accede a los medios virtuales.

1. Abra un explorador de web compatible en la estación de administración.
2. Inicie sesión en la interfaz Web del iDRAC6.
3. Haga clic en la ficha **Consola / Medios**.

   Aparecerá la pantalla **Redirección de consola y Medios virtuales**.

   Para cambiar los valores de cualquiera de los atributos mostrados, consulte "Configuración de los medios virtuales".

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

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

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

4. Haga clic en **Iniciar el visor**.

   NOTA: En Linux, el archivo **jviewer.jnlp** se descarga en el escritorio y un cuadro de diálogo preguntará qué desea hacer con el archivo. Elija la opción de **Abrir con el programa** y después seleccione la aplicación **javaws**, que se encuentra en el subdirectorio **bin** del directorio de instalación de JRE.

   La aplicación **iDRACView** se ejecuta en una ventana por separado.

5. Seleccione **Medios** → **Asistente de medios virtuales...**

   Aparecerá el **Asistente de redirección de medios**.

6. Abra la ventana **Estado** en la parte inferior de la pantalla **Asistente**. Si hay algún medio conectado, deberá desconectarlo antes de conectar otro medio. Para desconectar medios, haga clic en el botón **Desconectar** situado junto al medio en la ventana **Estado**.
7. Seleccione el botón de radio que está junto a los tipos de medios que desea conectar.

Puede seleccionar el botón de radio **Imagen de disco flexible** y uno de los botones de radio de la sección **Unidad de CD/DVD**.

Para conectar una imagen de disco flexible o una imagen ISO, introduzca la ruta de acceso a la ubicación de la imagen en la computadora local o haga clic en el botón **Examinar** para desplazarse hasta la ubicación de la imagen.

8. Haga clic en el botón **Conectar que se encuentra junto a cada tipo de medio seleccionado.**

   Los medios se conectan y la ventana **Estado** se actualiza.

9. Haga clic en **Cerrar.**

Desconexión de los medios virtuales

1. Seleccione **Medios** → **Asistente de medios virtuales...**

   Aparecerá el **Asistente de redirección de medios**.

2. Haga clic en **Desconectar** junto al medio que desea desconectar.

   El medio se desconectará y se actualizará la ventana **Estado.**

3. Haga clic en **Cerrar**.

Inicio desde los medios virtuales

El BIOS de sistema le permite iniciar desde unidades ópticas virtuales o desde unidades de disquete virtuales. Durante la POST, ingrese a la ventana de configuración del BIOS y verifique que las unidades virtuales estén activadas y que aparezcan en el orden correcto.

Para cambiar el valor en el BIOS, realice los pasos a continuación:

1. Inicie el servidor administrado.

2. Presione <F2> para ingresar a la ventana de configuración del BIOS.

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

   En la ventana emergente, aparece una lista de las unidades virtuales ópticas y de disco flexible virtuales con otros dispositivos normales de inicio.

4. Asegúrese que la unidad virtual esté activada y que aparezca como el primer dispositivo con medio iniciable. Si es necesario, siga las instrucciones que aparecen en la pantalla para modificar el orden de inicio.

5. Guarde los cambios y salga.

   El servidor administrado se reinicia.

   El servidor administrado intenta iniciarse a partir de un dispositivo iniciable con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio iniciable está presente, el sistema se iniciará a partir del dispositivo virtual. De lo contrario, el sistema ignorará el dispositivo; como ocurriría con un dispositivo físico que no tiene medios iniciables.

Instalación de sistemas operativos mediante medios virtuales

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

1. Verifique lo siguiente:
   - El DVD/CD de instalación de sistema operativo está insertado en la unidad de DVD/CD de la estación de administración.
   - La unidad de DVD/CD local está seleccionada.
   - Está conectado a las unidades virtuales.

2. Siga los pasos para iniciar desde los medios virtuales que aparecen en la sección "Inicio desde los medios virtuales" para asegurarse de que el BIOS esté configurado para que inicie desde la unidad de DVD/CD a partir de la que se realiza la instalación.

3. Siga las instrucciones en la pantalla para completar la instalación.

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

Sistemas con Windows

En sistemas con Windows, las unidades de medios virtuales se montan automáticamente cuando están conectadas y se configuran con una letra de unidad.

La utilización de las unidades virtuales desde el interior de Windows es similar a la utilización de las unidades físicas. Cuando se conecta a los medios por medio del asistente de medios virtuales, los medios estarán disponibles en el sistema cuando se haga clic en la unidad y se examine el contenido de la misma.

Sistemas con Linux

En función de la configuración del software del sistema, es posible que las unidades de medios virtuales no se monten automáticamente. Si las unidades no se montan automáticamente, monte manualmente las unidades con el comando **mount** de Linux.

Preguntas frecuentes

La tabla 12-3 contiene las preguntas y respuestas frecuentes.

Tabla 12-3. Uso de los medios virtuales: preguntas frecuentes

Pregunta	Respuesta
Algunas veces noto que mi conexión de cliente de medios virtuales se cierra. ¿Por qué?	Cuando se agota el tiempo de espera de la red, el firmware de iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Si los valores de configuración de los medios virtuales se cambian en la interfaz web del iDRAC6 o con los comandos de RACADM local, se desconectarán todos los medios conectados al momento de aplicar el cambio de configuración. Para restablecer la conexión con la unidad virtual, use el asistente de medios virtuales.
¿Qué sistemas operativos son compatibles con el iDRAC6?	Consulte "Sistemas operativos admitidos" para ver una lista de los sistemas operativos compatibles.
¿Qué exploradores web son compatibles con el iDRAC6?	Consulte "Exploradores web admitidos" para ver una lista de los exploradores de web admitidos.
¿Por qué a veces se pierde mi conexión de cliente?	• Algunas veces, puede perder la conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si cambia el CD en la unidad de CD del sistema cliente, en nuevo CD podría tener una función de inicio automático. Si éste es el caso, el firmware puede agotar el tiempo de espera y se puede perder la conexión cuando el sistema cliente tarda demasiado en estar listo para leer el CD. Si la conexión se cierra, vuelva a conectarla desde la interfaz gráfica de usuario y continúe con la operación anterior. • Cuando se agota el tiempo de espera de la red, el firmware de iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Asimismo, alguien puede haber cambiado los valores de configuración de los medios virtuales en la interfaz web o mediante comandos de RADACM. Para restablecer la conexión con el disco virtual, use la función de **Medios virtuales**.
La instalación del sistema operativo Windows parece tardar demasiado. ¿Por qué?	Si va a instalar el sistema operativo Windows con el CD *Dell PowerEdge Installation and Server Management* y una conexión de red lenta, el procedimiento de instalación puede requerir un tiempo prolongado para acceder a la interfaz web del iDRAC6 debido a la latencia de la red. Mientras la ventana de instalación no indique el progreso de la instalación, significa que el procedimiento de instalación está en progreso.
Veo el contenido de una unidad de disco flexible o memoria USB. Si trato de establecer una conexión de medios virtuales con la misma unidad, recibo un mensaje de error de conexión y se me pide que vuelva a intentarlo. ¿Por qué?	No se permite el acceso simultáneo a las unidades de disco flexible virtual. Cierre la aplicación que se utiliza para ver el contenido de la unidad antes de que intente hacer virtual la unidad.
¿Cómo configuro mi dispositivo virtual como dispositivo iniciable?	En el servidor administrado, acceda a la configuración del BIOS y vaya al menú de inicio. Localice el CD virtual, el disco flexible virtual o la memoria flash virtual y cambie el orden de dispositivo de inicio según corresponda. Por ejemplo, para iniciar a partir de una unidad de CD, configure la unidad de CD como la primera unidad en el orden de inicio.
¿A partir de qué tipos de medios puedo iniciar el sistema?	El iDRAC6 permite iniciar a partir de los medios iniciables siguientes: • Medios de CDROM/DVD de datos • Imagen ISO 9660 • Imagen de disco flexible o disco flexible de 1,44 pulgadas • Una memoria USB que el sistema operativo reconozca como disco extraíble (tamaño mínimo de 128 MB) • Una imagen de memoria USB
¿Cómo puedo hacer que mi memoria USB sea iniciable?	Busque en **support.dell.com** la utilidad Dell Boot Utility, un programa para Windows que se puede usar para hacer que la memoria USB de Dell funcione como dispositivo de inicio. Usted puede iniciar también con un disco de arranque de Windows 98 y copiar los archivos de sistema del disco de arranque a la memoria USB. Por ejemplo, desde una ventana del símbolo del sistema DOS, introduzca el comando siguiente:

	sys a: *x*: /s donde *x*: es la memoria USB que desea hacer iniciable. También puede usar la utilidad de inicio de Dell para crear una memoria USB iniciable. Esta utilidad sólo es compatible con las memorias USB de marca Dell. Para descargar la utilidad, abra un explorador de web, navegue al sitio web de asistencia Dell Support que se encuentra en **support.dell.com** y busque **R122672.exe**.
No puedo encontrar el dispositivo de disco flexible virtual en un sistema que ejecuta el sistema operativo Red Hat® Enterprise Linux® o SUSE® Linux. Mis medios virtuales están conectados y estoy conectado a mi disco flexible remoto. ¿Qué debo hacer?	Algunas versiones de Linux no montan automáticamente la unidad de disco flexible virtual y la unidad de CD virtual de manera similar. Para montar la unidad de disco flexible virtual, localice el nodo de dispositivo que Linux asigna a la unidad de disco flexible virtual. Ejecute los siguientes pasos para encontrar y montar correctamente la unidad de disco flexible virtual: 1. Abra una ventana del símbolo del sistema de Linux y ejecute el siguiente comando: grep "Disco flexible virtual" /var/log/messages 2. Localice la última anotación de dicho mensaje y anote la hora. 3. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: grep "*hh:mm:ss*" /var/log/messages donde: *hh:mm:ss* es la hora del mensaje que el comando grep informó en el paso 1. 4. En el paso 3, lea el resultado del comando grep y localice el nombre del dispositivo que se asigna al disco virtual Dell. 5. Asegúrese que está conectado a la unidad de disco flexible virtual. 6. En la ventana del símbolo del sistema de Linux, ejecute el siguiente comando: mount */dev/sdx* /mnt/floppy donde: */dev/sdx* es el nombre de dispositivo que se encontró en el paso 4 /mnt/floppy es el punto de montaje.
¿Qué tipo de sistemas de archivos son compatibles con mi unidad de disco virtual?	Su unidad de disco virtual es compatible con sistemas de archivos FAT16 o FAT32.
Cuando ejecuté una actualización de firmware de manera remota por medio de la interfaz web de iDRAC6, mis unidades virtuales en el servidor se desmontaron. ¿Por qué?	Las actualizaciones de firmware hacen que el iDRAC6 se restablezca, que abandone la conexión remota y que desmonte las unidades virtuales. Las unidades volverán a aparecer cuando el restablecimiento del iDRAC6 termine.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de RACADM local

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

La interfaz de línea de comando (CLI) de RACADM local brinda acceso a las funciones de administración del iDRAC6 desde el servidor administrado. RACADM brinda acceso a las mismas funciones que la interfaz web del iDRAC6. Sin embargo, RACADM se puede usar con secuencias de comandos para facilitar la configuración de varios servidores y controladores iDRAC, mientras que la interfaz web es más útil para la administración interactiva.

Los comandos de RACADM local no usan las conexiones de red para acceder al iDRAC6 desde el servidor administrado. Esto significa que usted puede usar comandos de RACADM local para configurar el sistema inicial de red del iDRAC6.

Para obtener más información sobre cómo configurar varios iDRAC, consulte "Configuración de varios iDRAC".

En esta sección se proporciona la información siguiente:

- Uso de RACADM desde una petición de comandos
- Configuración de iDRAC6 por medio del comando **racadm**
- Uso del archivo de configuración de RACADM para configurar varios iDRAC

Uso del comando RACADM

Los comandos de RACADM se ejecutan de manera local (en el servidor administrado) desde una petición de comandos o petición de shell.

Inicie sesión en el servidor administrado, abra un shell de comandos e introduzca comandos de RACADM local en el formato siguiente:

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

Sin opciones, el comando RACADM muestra la información general de uso. Para mostrar la lista de subcomandos de RACADM, introduzca:

```
racadm help
```

La lista de subcomandos incluye todos los comandos compatibles con el iDRAC6.

Para obtener ayuda para un subcomando, introduzca:

```
racadm help <subcomando>
```

El comando muestra la sintaxis y las opciones de línea de comandos del subcomando.

Subcomandos de RACADM

La tabla 13-1 Proporciona una descripción de cada uno de los subcomandos de RACADM que se pueden ejecutar en RACADM. Para ver una lista detallada de los subcomandos de RACADM que incluye la sintaxis y las anotaciones válidas, consulte "Generalidades del subcomando RACADM".

Tabla 13-1. Subcomandos de RACADM

Comando	Descripción
clrasrscreen	Borra la pantalla de último bloqueo (ASR)
clrraclog	Borra el registro de iDRAC6. Después de borrarlo, sólo se hace una anotación para indicar el usuario que borró el registro y la hora en la que se borró.
clrsel	Borra las anotaciones del registro de sucesos del sistema del servidor administrado.
config	Configura el iDRAC6.
getconfig	Muestra las propiedades de configuración actuales del iDRAC6.
getniccfg	Muestra la configuración IP actual del controlador.
getraclog	Muestra el registro del iDRAC6.
getractime	Muestra la hora del iDRAC6.
getssninfo	Muestra información sobre las sesiones activas.
getsvctag	Muestra las etiquetas de servicio.
getsysinfo	Muestra información sobre el iDRAC6 y el servidor administrado, incluida la configuración de IP, el modelo de hardware, las versiones de firmware y la información del sistema operativo.

gettracelog	Muestra el registro de rastreo de iDRAC6. Si se usa con -i, el comando muestra el número de anotaciones en el registro de rastreo de iDRAC6.
help	Muestra una lista de subcomandos del iDRAC6.
help <*subcomando*>	Muestra la descripción de uso del subcomando especificado.
localconredirdisable	Desactiva el kVM local desde el sistema local.
racreset	Restablece la configuración del iDRAC6.
racresetcfg	Restablece la configuración predeterminada del iDRAC6.
serveraction	Realiza operaciones de administración de alimentación en el servidor administrado.
setniccfg	Establece la configuración IP para el controlador.
sslcertdownload	Descarga un certificado CA.
sslcertupload	Carga un certificado de CA o un certificado de servidor en el iDRAC6.
sslcertview	Muestra un certificado de CA o un certificado de servidor en el iDRAC6.
sslcsrgen	Genera y descarga la CSR de SSL.
testemail	Obliga al iDRAC6 a enviar un correo electrónico a través del NIC de iDRAC6.
testtrap	Obliga al iDRAC6 a enviar una alerta SNMP a través del NIC de iDRAC6.
vmkey	Restablece la clave multimedia virtual a su tamaño predeterminado de 256 MB.

Uso de la utilidad RACADM para configurar el iDRAC6

Esta sección describe cómo usar RACADM para realizar varias tareas de configuración del iDRAC6.

Visualización de la configuración actual del iDRAC6

El subcomando **getconfig** de RACADM obtiene los valores de configuración actuales del iDRAC6. Los valores de configuración se organizan en *grupos* que contienen uno o varios *objetos* y los objetos tienen *valores*.

Consulte "Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6" para ver una descripción completa de los grupos y objetos.

Para mostrar una lista de todos los grupos de iDRAC6, introduzca este comando:

```
racadm getconfig -h
```

Para mostrar los objetos y valores de un grupo en particular, introduzca este comando:

```
racadm getconfig -g <grupo>
```

Por ejemplo, para mostrar una lista de todos los valores del objeto de grupo **cfgLanNetworking**, introduzca el comando siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Administración de usuarios del iDRAC6 con RACADM

NOTA: Tenga precaución cuando utilice el comando **racresetcfg**, pues se restablecerán *todos* los parámetros de configuración predeterminados originales. Todos los cambios anteriores se perderán.

NOTA: Si está configurando un iDRAC6 nuevo o si ha ejecutado el comando **racadm racresetcfg**, el único usuario actual es **root** con la contraseña **calvin**.

NOTA: Los usuarios se pueden activar o desactivar posteriormente. Por consiguiente, un usuario puede tener un número de índice diferente en cada iDRAC6.

NOTA: Los usuarios y grupos creados para entornos de Active Directory deben cumplir con la convención de nombres de Active Directory.

Puede configurar hasta 15 usuarios en la base de datos de propiedades de iDRAC6. (El decimosexto usuario se reserva para el usuario de LAN de IPMI.) Antes de activar manualmente un usuario de iDRAC6, verifique si existe algún usuario actual.

Para verificar si existe un usuario, introduzca el comando siguiente en la petición de comandos:

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

O bien:

introduzca el comando siguiente una vez para cada índice de 1 a 16:

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

NOTA: También puede introducir racadm getconfig -f <*nombre_de_archivo*> y ver el archivo <*nombre-_de_archivo*> que se genera y que incluye a todos los usuarios, así como todos los demás parámetros de configuración del iDRAC6.

Se muestran varios parámetros e identificaciones de objetos con sus valores actuales. Los dos objetos de interés son:

```
# cfgUserAdminIndex=nn

cfgUserAdminUserName=
```

Si el objeto **cfgUserAdminUserName** no tiene un valor, el número de índice que indica el objeto **cfgUserAdminIndex** está disponible para su uso. Si aparece un nombre después del signo =, significa que ese índice está asignado a ese nombre de usuario.

NOTA: Los usuarios y grupos creados para entornos de Active Directory deben cumplir con la convención de nombres de Active Directory.

Incorporación de un usuario de iDRAC6

Para agregar un nuevo usuario al iDRAC6, realice los pasos siguientes:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca el privilegio de inicio de sesión en el iDRAC6 para el usuario.
4. Active el usuario.

Ejemplo

El ejemplo a continuación describe cómo agregar un nuevo usuario de nombre "Juan" con una contraseña "123456" y privilegios de inicio de sesión en el iDRAC6.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 juan

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

Para verificar el usuario nuevo, use uno de los comandos siguientes:

```
racadm getconfig -u juan

racadm getconfig -g cfgUserAdmin -i 2
```

Activación de un usuario del iDRAC6 con permisos

Para otorgar permisos administrativos específicos (en base a funciones) a un usuario, configure la propiedad **cfgUserAdminPrivilege** con una máscara de bits creada a partir de los valores que se muestran en la tabla 13-2:

Tabla 13-2. Máscaras de bit para privilegios del usuario

Privilegio del usuario	Máscara de bits de privilegios
Iniciar sesión en el iDRAC6	0x0000001
Configurar el iDRAC6	0x0000002
Configurar usuarios	0x0000004
Borrar registros	0x0000008
Ejecutar comandos de control del servidor	0x0000010
Acceder a redirección de consola	0x0000020
Acceder a los medios virtuales	0x0000040
Probar alertas	0x0000080
Ejecutar comandos de depuración	0x0000100

Por ejemplo, para permitir al usuario **Configurar el iDRAC**, **Configurar usuarios**, **Borrar registros** y **Acceder a la redirección de consola**, agregue los valores 0x00000002, 0x00000004, 0x00000008 y 0x00000010 para crear el mapa de bits 0x0000002E. Después introduzca el siguiente comando para establecer el privilegio:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i 2 0x0000002E
```

Eliminación de un usuario de iDRAC6

Al usar RACADM, los usuarios se deben desactivar manual e individualmente. Los usuarios no se pueden eliminar por medio de un archivo de configuración.

El ejemplo siguiente ilustra la sintaxis de comando que se puede usar para eliminar un usuario de RAC:

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

Una cadena nula de dos caracteres de comillas ("") indica al iDRAC6 que debe eliminar la configuración del usuario en el índice especificado y volver a establecer los valores predeterminados originales de fábrica en la configuración del usuario.

Pruebas de las alertas por correo electrónico

La función de alertas por correo electrónico del iDRAC6 permite a los usuarios recibir alertas por correo electrónico cuando se produce un suceso crítico en el servidor administrado. El siguiente ejemplo muestra cómo probar la función de alertas por correo electrónico para asegurarse de que el iDRAC6 pueda enviar correctamente alertas por correo electrónico a través de la red.

```
racadm testemail -i 2
```

NOTA: Asegúrese de que los valores de SMTP y de alerta por correo electrónico estén configurados antes de probar la función de alertas por correo electrónico. Consulte "Configuración de alertas por correo electrónico" para obtener más información.

Prueba de la función de alertas de capturas SNMP del iDRAC6

La función de envío de alertas de capturas SNMP del iDRAC6 permite que las configuraciones de oyentes de capturas SNMP reciban capturas de los sucesos de sistema que se presentan en el servidor administrado.

El ejemplo a continuación muestra cómo un usuario puede probar la función de alertas de capturas SNMP.

```
racadm testtrap -i 2
```

NOTA: Antes de probar la función de alertas de capturas SNMP del iDRAC6, asegúrese de que los valores de captura y SNMP estén configurados correctamente. Consulte las descripciones de lo subcomandos **testtrap** y **testemail** para configurar estos valores.

Configuración de las propiedades de red del iDRAC6

Para generar una lista de las propiedades disponibles de red, introduzca lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

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

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

Los comandos proporcionan la misma funcionalidad de configuración que la utilidad de configuración de iDRAC6 cuando se le pide que pulse <Ctrl><E>. Para obtener más información sobre la configuración de las propiedades de red con la utilidad de configuración del iDRAC6, consulte "LAN de iDRAC6".

El siguiente es un ejemplo de cómo se pueden utilizar los comandos para configurar las propiedades de red LAN deseadas.

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

NOTA: Si **cfgNicEnable** se establece en **0**, la LAN de iDRAC6 se desactivará aun cuando DHCP esté activado.

Configuración de IPMI en la LAN

1. Configure la IPMI en la LAN con el comando siguiente:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
   ```

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

   a. Actualice los privilegios de canal de IPMI con el comando siguiente:

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

      donde <*nivel*> es uno de los siguientes valores:

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

      Por ejemplo, para establecer el privilegio de canal de LAN de IPMI en 2 (usuario), introduzca el comando siguiente:

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
      ```

   b. De ser necesario, defina la clave de cifrado del canal de la LAN de IPMI con un comando como el siguiente:

NOTA: La IPMI de iDRAC6 es compatible con el protocolo RMCP+. Consulte las especificaciones de IPMI 2.0 para obtener más información.

      ```
      racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clave>
      ```

      donde <*clave*> es una clave de cifrado de 20 caracteres en un formato hexadecimal válido.

2. Configure la comunicación en serie en la LAN (SOL) con el comando siguiente:

   ```
   racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
   ```

NOTA: El nivel de privilegios mínimo de SOL de IPMI determina los privilegios mínimos que se requieren para activar la SOL de IPMI. Para obtener más información, consulte la especificación IPMI 2.0.

   a. Actualice el nivel mínimo de privilegio de la SOL de IPMI con el comando siguiente:

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <nivel>
      ```

      donde <*nivel*> es uno de los siguientes:

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

      Por ejemplo, para definir los privilegios de IPMI como 2 (Usuario), introduzca el comando siguiente:

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
      ```

NOTA: Para redirigir la consola de serie en la LAN, asegúrese de que la velocidad en baudios de la comunicación en serie en la LAN sea idéntica a la velocidad en baudios del sistema administrado.

   b. Actualice la velocidad en baudios de la SOL de IPMI con el comando siguiente:

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <velocidad_en_baudios>
      ```

      donde <*velocidad_en_baudios*> es 19200, 57600 o 115200 bps.

      Por ejemplo:

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
      ```

   c. Active la comunicación en serie en la LAN escribiendo el comando siguiente en la petición de comandos.

NOTA: Cada usuario individual puede activar o desactivar la SOL.

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

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

Configuración del PEF

Puede configurar la acción que desea que el iDRAC6 ejecute ante cada alerta de plataforma. La tabla 13-3 muestra las acciones posibles y el valor para

identificarlas en RACADM.

Tabla 13-3. Acción de sucesos de plataforma

Acción	Valor
Sin acción	0
Está apagado	1
Reiniciar	2
Ciclo de encendido	3

1. Configure acciones de filtro de sucesos de plataforma con el comando siguiente:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <índice> <valor_de_acción>
   ```

   donde <*índice*> es el índice de filtro de sucesos de plataforma (tabla 5-7) y <*valor_de_acción*> es un valor de la tabla 13-3.

   Por ejemplo, para hacer que el filtro de sucesos de plataforma reinicie el sistema y envíe una alerta de IPMI cuando se detecte un suceso crítico del procesador, introduzca el siguiente comando:

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2
   ```

Configuración de la PET

1. Active las alertas globales con el comando siguiente:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active la captura de sucesos de plataforma con el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <índice> <0|1>
   ```

   donde <*índice*> es el índice de destino de la captura de sucesos de plataforma y `0` o `1` desactiva o activa la captura de sucesos de plataforma, respectivamente.

   Por ejemplo, para activar una PET con índice 4, introduzca el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1
   ```

3. Configure la política de captura de sucesos de plataforma con el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <índice> <dirección_IP>
   ```

   donde *índice* es el índice del destino de la captura de sucesos de plataforma y <*dirección_IP*> es la dirección IP de destino del sistema que recibe las alertas de sucesos de plataforma.

4. Configure la cadena de nombre de comunidad.

   En el indicador de comandos, introduzca:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <nombre>
   ```

   donde <*nombre*> es el nombre de comunidad de la captura de sucesos de plataforma.

Configuración de alertas por correo electrónico

1. Active las alertas globales con el comando siguiente:

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
   ```

2. Active las alertas por correo electrónico con los comandos siguientes:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i <índice> <0|1>
   ```

   donde <*índice*> es el índice del destino de correo electrónico y 0 desactiva la alerta por correo electrónico o 1 activa la alerta. El índice de destino de correo electrónico puede ser un valor de 1 a 4.

   Por ejemplo, para activar un correo electrónico con índice 4, introduzca el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. Configure los valores de correo electrónico con el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <dirección_de_correo_electrónico>
   ```

   donde 1 es el índice del destino del mensaje de correo electrónico y <*dirección_de_correo_electrónico*> es la dirección de correo electrónico de destino que recibe las alertas de sucesos de plataforma.

4. Para configurar un mensaje personalizado, introduzca el comando siguiente:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <índice> <mensaje_personalizado>
   ```

   donde *índice* es el índice del destino del mensaje de correo electrónico y <*mensaje_personalizado*> es el mensaje personalizado.

5. Si lo desea, pruebe la alerta configurada de correo electrónico con el comando siguiente:

   ```
   racadm testemail -i <índice>
   ```

   donde <*índice*> es el índice del destino de correo electrónico que va a probar.

Configuración de la filtración de IP (IP Range)

La filtración de direcciones IP (o *Comprobación de rango de IP*) permite el acceso al iDRAC6 únicamente a los clientes o estaciones de administración cuyas direcciones IP estén dentro de un rango especificado por el usuario. Todas las demás solicitudes de inicio de sesión son denegadas.

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP que se especifica en las siguientes propiedades de **cfgRacTuning**:

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propiedad **cfgRacTuneIpRangeMask** se aplica a la dirección IP entrante y a las propiedades **cfgRacTuneIpRangeAddr**. Si los resultados son idénticos, se permite que la petición de inicio de sesión entrante tenga acceso al iDRAC6. Los inicios de sesión provenientes de direcciones IP fuera de este rango recibirán un mensaje de error.

El inicio de sesión procederá si el valor de la siguiente expresión es igual a cero:

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

donde & es el operador Y a nivel de bits de las cantidades y ^ es el operador O exclusivo a nivel de bits.

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

Tabla 13-4. Propiedades del filtrado de direcciones IP (IPRange)

Propiedad	Descripción
cfgRacTuneIpRangeEnable	Activa la función de comprobación de rango de IP.
cfgRacTuneIpRangeAddr	Determina el patrón de bits de la dirección IP aceptable, en función de los números 1 de la máscara de subred. Esta propiedad se basa en el modo en bits y *AND* con **cfgRacTuneIpRangeMask** para determinar la parte superior de la dirección IP permitida. Se permite que cualquier dirección IP que contenga este patrón de bits en los bits superiores inicie sesión. Los inicios de sesión que provengan de las direcciones de IP estén fuera de este rango fallarán. Los valores predeterminados en cada propiedad permiten que el rango de direcciones de 192.168.1.0 a 192.168.1.255 inicien sesión.
cfgRacTuneIpRangeMask	Define las posiciones significativas de bit en la dirección IP. La máscara debe darse en forma de máscara de red, donde todos los bits más significativos son unos (1) con una sola transición total a ceros en los bits del orden inferior.

Configuración de la filtración de IP

Para configurar la filtración de IP en la interfaz web, siga estos pasos:

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Red/Seguridad**.
2. En la pantalla **Configuración de red**, haga clic en **Configuración avanzada**.
3. Marque la casilla **Rango IP activado** e introduzca la **Dirección de rango IP** y la **Máscara de subred de rango IP**.
4. Haga clic en **Aplicar**.

A continuación se presentan ejemplos de cómo usar RACADM local para configurar la filtración de IP.

NOTA: Consulte "Uso de la interfaz de línea de comandos de RACADM local" para obtener más información sobre RACADM y los comandos RACADM.

1. Los siguientes comandos RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57:

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

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
   ```

2. Para restringir los inicios de sesión a un pequeño conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo salvo los últimos dos bits de la máscara, según se muestra a continuación:

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

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

   racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
   ```

   El último byte de la máscara de rango está establecido como 252, el equivalente decimal de 11111100b.

Directrices para el filtrado de IP

Utilice las directrices a continuación cuando active el filtrado de IP:

- Compruebe que **cfgRacTuneIpRangeMask** esté configurado en forma de máscara de red, donde los bits más significativos son los números 1 (que definen la subred en la máscara) con una transición a sólo ceros en los bits de nivel inferior.
- Use la dirección base del rango deseado como el valor de **cfgRacTuneIpRangeAddr**. El valor binario de 32 bits de esta dirección debe tener ceros en todos los bits de orden inferior donde hay ceros en la máscara.

Configuración del bloqueo de IP

El bloqueo de IP detecta de forma dinámica cuando se presentan fallas de inicio de sesión provenientes de una dirección IP específica y bloquea (o impide) el inicio de sesión de dicha dirección en el iDRAC6 durante un lapso de tiempo predefinido.

Las funciones del bloqueo de IP incluye:

- El número de fallas permitidas de inicio de sesión (**cfgRacTuneIpBlkFailcount**)
- El periodo en segundos durante el cual se deben presentar estas fallas (**cfgRacTuneIpBlkFailWindow**)
- La cantidad de tiempo en segundos durante el que se impide que la dirección IP bloqueada establezca una sesión después de haber excedido el número de fallas permitidas (**cfgRacTuneIpBlkPenaltyTime**)

Conforme se acumulan las fallas de inicio de sesión provenientes de una dirección IP específica, un contador interno lleva registro de las mismas. Cuando el usuario inicia sesión satisfactoriamente, el historial de intentos fallidos se borra y el contador interno se restablece.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje: ssh exchange identification: Connection closed by remote host. (Identificación de intercambio de SSH: el host remoto cerró la conexión).

Consulte "Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6" para ver una lista completa de las propiedades de **cfgRacTune**.

"Propiedades de restricción (Bloqueo de IP) de reintentos de inicio de sesión" muestra una lista de los parámetros definidos por el usuario.

Tabla 13-5. Propiedades de restricción (Bloqueo de IP) de reintentos de inicio de sesión

Propiedad	Definición
cfgRacTuneIpBlkEnable	Activa la función de bloqueo de IP. Cuando se presenten fallas consecutivas (**cfgRacTuneIpBlkFailCount**) provenientes de una única dirección IP dentro de lapso de tiempo específico (**cfgRacTuneIpBlkFailWindow**), todos los intentos posteriores de establecimiento de sesión que provengan de dicha dirección serán rechazados durante un período de tiempo determinado (**cfgRacTuneIpBlkPenaltyTime)**.
cfgRacTuneIpBlkFailCount	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión.
cfgRacTuneIpBlkFailWindow	El periodo en segundos durante el cual se cuentan los intentos fallidos. Cuando los intentos fallidos superan este límite, se eliminan del contador.
cfgRacTuneIpBlkPenaltyTime	Define el período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas.

Activación del bloqueo de IP

El ejemplo siguiente impide a una dirección IP cliente establecer una sesión durante cinco minutos si dicho cliente ha fallado cinco intentos de inicio de sesión en un período de un minuto.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

El ejemplo siguiente evita más de tres intentos fallidos dentro de un minuto y evita los intentos de inicio adicionales durante una hora.

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

Configuración de los servicios de Telnet y SSH del iDRAC6 por medio de RACADM local

La consola de Telnet/SSH se puede configurar de manera local (en el servidor administrado) con los comandos de RACADM.

NOTA: Se debe tener permiso de **Configurar el iDRAC6** para ejecutar los comandos en esta sección.

NOTA: Cuando usted reconfigura los valores de Telnet o SSH en el iDRAC6, todas las sesiones actuales se terminan sin advertencia.

Para activar Telnet y SSH desde RACADM local, inicie sesión en el servidor administrado e introduzca los siguientes comandos en el símbolo de sistema:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Para desactivar el servicio Telnet o SSH, cambie el valor de `1` a `0`:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0

racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Introduzca el siguiente comando para cambiar el número de puerto de Telnet en el iDRAC6:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <número del nuevo puerto>
```

Por ejemplo, para cambiar el puerto Telnet del valor predeterminado 22 a 8022, introduzca este comando:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

Para ver una lista completa de los comandos disponibles de la CLI de RACADM, consulte "Uso de la interfaz de línea de comandos de RACADM local".

Uso de un archivo de configuración de iDRAC6

El archivo de configuración de iDRAC6 es un archivo de texto que contiene una representación de los valores en la base de datos de iDRAC6. Puede usar el subcomando **getconfig** de RACADM para generar un archivo de configuración que contenga los valores actuales del iDRAC6. Puede modificar entonces el archivo y usar el subcomando **config -f** de RACADM para cargar el archivo nuevamente en el iDRAC6 o para copiar la configuración a otros iDRAC.

Creación de un archivo de configuración de iDRAC6

El archivo de configuración es un archivo de texto simple. Se puede usar cualquier nombre de archivo válido; sin embargo, la convención recomendada es la extensión de archivo **.cfg**.

El archivo de configuración se puede:

- Crear con un editor de textos
- Obtenerse del iDRAC6 con el subcomando **getconfig** de RACADM
- Obtenerse del iDRAC6 con el subcomando **getconfig** de RACADM y después editarse

Para obtener un archivo de configuración, con el comando **getconfig** de RACADM, introduzca el comando siguiente en la petición de comandos del servidor administrado:

```
racadm getconfig -f myconfig.cfg
```

Este comando crea el archivo **myconfig.cfg** en el directorio actual.

Sintaxis del archivo de configuración

NOTA: Modifique el archivo de configuración con un editor de textos sin formato, como el **Bloc de notas** en Windows o **vi** en Linux. La utilidad **racadm** analiza únicamente el texto ASCII. Los formatos confunden al analizador y pueden dañar la base de datos de iDRAC6.

Esta sección describe el formato del archivo de configuración.

- **Las líneas que comienzan con # son comentarios.**

  Un comentario *debe* comenzar en la primera columna de la línea. Un carácter # que esté en cualquier otra columna será tratado como carácter # normal.

  Ejemplo:

  ```
  #

  # This is a comment (Esto es un comentario)

  [cfgUserAdmin]

  cfgUserAdminPrivilege=4
  ```

- Todas las anotaciones de grupo deben estar encerradas en los caracteres ***[*** y ***]***.

  El carácter inicial ***[*** que denota un nombre de grupo *debe* iniciar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de configuración se organizan en grupos según se define en "Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6".

  El siguiente ejemplo muestra un nombre de grupo, el objeto y el valor de propiedad del objeto.

  Ejemplo:

  ```
  [cfgLanNetworking] (nombre de grupo)

  cfgNicIpAddress=143.154.133.121 (nombre de objeto)
  ```

- Todos los parámetros se especifican como pares *objeto=valor* sin espacio en blanco entre el objeto, el signo "=" y el valor.

  El espacio en blanco que se incluye después del valor se ignora. El espacio en blanco dentro de una cadena de valores no se modifica. Todo carácter a la derecha del signo = se toma tal cual es (por ejemplo, un segundo = o un #, *[*, *]*, etc.).

- El analizador ignora una anotación de objeto de índice.

  El usuario *no puede* especificar qué índice se va a usar. Si el índice ya existe, se utiliza, o bien, se crea la nueva anotación en el primer índice disponible de dicho grupo.

  El comando `racadm getconfig -f <nombre_de_archivo>` coloca un comentario frente a los objetos del índice, lo que permite ver los comentarios que se incluyen.

  NOTA: Usted puede crear un grupo indexado manualmente con el siguiente comando:
  racadm config -g <*nombre_de_grupo*> -o <*objeto anclado*> -i <*índice*> <*nombre-de-ancla-exclusivo*>.

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

  El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

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

  NOTA: Una cadena NULA (que se identifica por dos caracteres "") indica al iDRAC6 que elimine el índice del grupo especificado.

  Para ver el contenido de un grupo indexado, use el siguiente comando:

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

- Para grupos indexados, el ancla de objeto *debe ser* el primer objeto después del par *[ ]*. Los siguientes son ejemplos de los grupos indexados actuales:

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<nombre_de_usuario>
  ```

- Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.

  El analizador lee en todos los índices de iDRAC6 para ese grupo. Los objetos dentro de dicho grupo son modificaciones simples cuando se configura el iDRAC6. Si un objeto modificado representa un índice nuevo, el índice se crea en el iDRAC6 durante la configuración.

- No se puede especificar un índice deseado en un archivo de configuración.

  Los índices se pueden crear y eliminar, por lo que con el tiempo el grupo se puede fragmentar con índices usados y no usados. Si hay un índice presente, éste es modificado. Si no hay un índice presente, se usa el primer índice disponible. Este método permite tener flexibilidad al momento de agregar anotaciones indexadas en las que usted no necesita hacer coincidencias exactas de índice entre todos los RAC que se administran. Se agregan nuevos usuarios al primer índice disponible. Es posible que un archivo de configuración que se analiza y se ejecuta correctamente en un iDRAC6 no funcione correctamente en otro si todos los índices están llenos y usted tiene que agregar un nuevo usuario.

Modificación de la dirección IP del iDRAC6 en un archivo de configuración

Cuando modifique la dirección IP del iDRAC6 en el archivo de configuración, elimine todas las anotaciones de **<***variable***>=**<*valor*> innecesarias. Sólo la etiqueta variable real del grupo con "[" y "]" permanecerá, incluyendo las dos anotaciones **<***variable***>**=<*valor*> relacionadas con el cambio de la dirección IP.

Por ejemplo:

```
#

# Object Group (Grupo de objeto) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Este archivo será actualizado de la siguiente manera:

```
#

# Object Group (Grupo de objeto) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

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

cfgNicGateway=10.35.9.1
```

Carga del archivo de configuración en el iDRAC6

El comando `racadm config -f <nombre_de_archivo>` analiza el archivo de configuración para verificar que el grupo y los nombres de objeto válidos estén presentes y que se cumpla con las reglas de la sintaxis. Si el archivo no tiene errores, el comando actualizará la base de datos del iDRAC6 con el contenido del archivo.

NOTA: Para verificar únicamente la sintaxis y no actualizar la base de datos del iDRAC6, agregue la opción **-c** al subcomando **config**.

Los errores dentro del archivo de configuración se señalan con el número de línea y un mensaje que explica el problema. Usted deberá corregir todos los errores antes de que el archivo de configuración se pueda actualizar en el iDRAC6.

NOTA: Use el subcomando **racresetcfg** para restablecer la base de datos y la configuración predeterminada original de la tarjeta de interfaz de red de iDRAC6 y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario "root" está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Antes ejecutar el comando `racadm config -f <nombre_de_archivo>`, puede ejecutar el subcomando `racresetcfg` para restablecer la configuración predeterminada del iDRAC6. Asegúrese de que el archivo que se va a cargar incluya todos los objetos, usuarios, índices y otros parámetros deseados.

Para actualizar el iDRAC6 con el archivo de configuración, ejecute el comando siguiente en la petición de comandos del servidor administrado:

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

Después de que el comando ha terminado, usted puede ejecutar el subcomando **getconfig** de RACADM para confirmar que la actualización fue satisfactoria.

Configuración de varios iDRAC

A través de un archivo de configuración, usted puede configurar otros iDRAC con propiedades idénticas. Siga estos pasos para configurar varios iDRAC:

1. Cree el archivo de configuración del iDRAC6 cuyos valores desea copiar en los demás. En una petición de comandos del servidor administrado, introduzca el comando siguiente:

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

   donde <*nombre_de_archivo*> es el nombre de un archivo para guardar las propiedades del iDRAC6, como **myconfig.cfg**.

   Consulte "Creación de un archivo de configuración de iDRAC6" para obtener más información.

   NOTA: Algunos archivos de configuración contienen información exclusiva de iDRAC6 (como la dirección IP estática) que se debe modificar antes de exportar el archivo a otros iDRAC.

2. Modifique el archivo de configuración que ha creado en el paso anterior y quite o marque como comentarios los valores que *no desea* reproducir.

3. Copie el archivo de configuración modificado en una unidad de red donde esté disponible para cada servidor administrado cuyo iDRAC6 desea configurar.

4. Para cada iDRAC6 que desea configurar:

   a. Inicie sesión en el servidor administrado y abra una petición de comandos.

   b. Si desea cambiar la configuración predeterminada del iDRAC6, introduzca el comando siguiente:

      ```
      racadm racreset
      ```

   c. Cargue el archivo de configuración en el iDRAC6 con el comando siguiente:

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

      donde <*nombre_de_archivo*> es el nombre del archivo de configuración que ha creado. Incluya la ruta de acceso completa si el archivo no está en el directorio de trabajo.

   d. Restablezca el iDRAC6 que se configuró por medio del comando siguiente:

      ```
      racadm reset
      ```

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de SM-CLP de iDRAC6

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Esta sección ofrece información acerca del Protocolo de línea de comandos de administración de servidor (SM-CLP) del Grupo de trabajo de administración de servidor (SMWG) que está incorporado en el iDRAC6.

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

El SM-CLP de iDRAC6 es un protocolo impulsado por el DMTF y el SMWG para proporcionar estándares para las implementaciones de la interfaz de línea de comandos para administración de sistemas. Se están realizando muchos esfuerzos para obtener una arquitectura SMASH definida como punto de partida para un conjunto de componentes de administración de sistemas más estandarizado. El SM-CLP de SMWG es un subcomponente de los esfuerzos generales de SMASH realizados por DMTF.

El SM-CLP ofrece un subconjunto de funciones de la interfaz de línea de comandos de RACADM local, pero con una ruta de acceso distinta. SM-CLP se ejecuta dentro del iDRAC6, mientras que RACADM se ejecuta en el servidor administrado. Asimismo, RACADM es una interfaz patentada de Dell; SM-CLP es una interfaz estándar de la industria. Consulte "Equivalencias de RACADM y SM-CLP" para ver una relación de los comandos RACADM y SM-CLP.

Administración del sistema con SM-CLP

El SM-CLP del iDRAC6 permite administrar las siguientes funciones del sistema desde una línea de comandos o una secuencia de comandos:

- Administración de la alimentación de servidor: enciende, apaga o reinicia el sistema
- Administración de registro de sucesos del sistema: muestra o borra las anotaciones del registro de sucesos del sistema
- Administración de cuentas de usuario del iDRAC6
- Configuración de Active Directory
- Configuración de la LAN de iDRAC6
- Generación de solicitudes de firma de certificados (CSR) de SSL
- Configuración de los medios virtuales
- Redirección de la comunicación en serie en la LAN (SOL) por medio de Telnet o SSH

Compatibilidad con SM-CLP de iDRAC6

SM-CLP se aloja en el firmware del iDRAC6 y es compatible con conexiones de Telnet y SSH. La interfaz de SM-CLP de iDRAC6 está basada en la versión 1.0 de la especificación SM-CLP proporcionada por la organización DMTF.

Las siguientes secciones proporcionan una descripción de la característica de SM-CLP que se aloja en el iDRAC6.

Funciones de SM-CLP

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

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

A continuación se presenta la sintaxis de la línea de comandos de SM-CLP:

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

La tabla 14-1 muestra una lista de los verbos compatibles con la CLI del iDRAC6, la sintaxis de cada comando y una lista de las opciones compatibles con los verbos.

Tabla 14-1. Verbos compatibles con la CLI de SM-CLP

Verbo	Descripción	Opciones
cd	Navega por el espacio de direcciones de sistema administrado por medio del shell. Sintaxis: cd [*opciones*] [*destino*]	-default, -examine, -help, -output, -version
delete	Elimina un objeto. Sintaxis: delete [*opciones*] *destino*	-examine, -help, -output, -version
dump	Lleva una imagen binaria del punto de acceso de administrabilidad a un URI. dump -destination <*URI*> [*opciones*] [*destino*]	-destination, -examine, -help, -output, -version
exit	Cierra la sesión de shell de SM-CLP. Sintaxis: exit [*opciones*]	-help, -output, -version
help	Muestra la ayuda de los comandos de SM-CLP. help	-examine, -help, -output, -version
load	Lleva una imagen binaria de un URI al punto de acceso de administrabilidad. Sintaxis: load -source <*URI*> [*opciones*] [*destino*]	-examine, -help, -output, -source, -version
reset	Restablece el destino. Sintaxis: reset [*opciones*] [*destino*]	-examine, -help, -output, -version
set	Establece las propiedades de un destino Sintaxis: set [*opciones*] [*destino*] <*nombre de propiedad*>=<*valor*>	-examine, -help, -output, -version
show	Muestra las propiedades, verbos y destinos secundarios del destino. Sintaxis: show [*opciones*] [*destino*] <*nombre de propiedad*>=<*valor*>	-all, -default, -display, -examine, -help, -level, -output, -version
start	Inicia un destino. Sintaxis: start [*opciones*] [*destino*]	-examine, -force, -help, -output, -version
stop	Desactiva un destino. Sintaxis: stop [*opciones*] [*destino*]	-examine, -force, -help, -output, -version, -wait
version	Muestra los atributos de versión de un destino. Sintaxis: version [*opciones*]	-examine, -help, -output, -version

La tabla 14-2 describe las opciones de SM-CLP. Algunas opciones tienen formas abreviadas, según se muestra en la tabla.

Tabla 14-2. Opciones admitidas por CM-CLP

Opción de SM-CLP	Descripción
-all, -a	Indica al verbo que realice todas las funciones posibles.
-destination	Especifica la ubicación para guardar una imagen en el comando dump. Sintaxis: -destination <URI>
-display, -d	Filtra la salida generada por el comando.

	Sintaxis: `-display <propiedades | destinos | verbos>[, <propiedades | destinos | verbos>]*`
-examine, -x	Indica al procesador de comandos que valide la sintaxis del comando sin ejecutarlo.
-help, -h	Muestra la ayuda del verbo.
-level, -l	Indica al verbo que se aplique a destinos en niveles adicionales por debajo del destino especificado. Sintaxis: `-level <n | all>`
-output, -o	Especifica el formato de la salida. Sintaxis: `-output <text | clpcsv | clpxml>`
-source	Especifica la ubicación de una imagen en un comando de carga. Sintaxis: `-source <URI>`
-version, -v	Muestra el número de versión de SMASH-CLP.

Navegación del espacio de direcciones de MAP

NOTA: La diagonal (/) y la diagonal invertida (\) pueden intercambiarse en las rutas de acceso de direcciones en SM-CLP. Sin embargo, una diagonal invertida al final de una línea de comandos hace que el comando continúe en la línea siguiente y se ignora cuando el comando se ejecuta.

Los objetos que pueden ser administrados con SM-CLP se representan con destinos organizados en un espacio jerárquico denominado espacio de direcciones de Punto de acceso de administrabilidad (MAP). La ruta de acceso de la dirección especifica la ruta de acceso desde la raíz del espacio de direcciones hacia un objeto en el espacio de direcciones.

El destino raíz se representa con una diagonal (/) o una diagonal invertida (\). Es el punto de partida predeterminado cuando se inicia sesión en el iDRAC6. Vaya hacia la raíz con el verbo cd. Por ejemplo, para navegar a la tercera anotación en el Registro de sucesos del sistema (SEL), introduzca el comando siguiente:

```
->cd /system1/sp1/logs1/record3
```

Introduzca el verbo cd sin destino para encontrar la ubicación actual en el espacio de direcciones. Las abreviaturas `..` y `.` funcionan de la misma forma que en Windows y Linux: `..` se refiere al nivel superior inmediato y `.` se refiere al nivel actual.

Destinos

La tabla 14-3 muestra una lista de destinos disponibles por medio de SM-CLP.

Tabla 14-3. Destinos de SM-CLP

Destino	Definición
/system1/	El destino de sistema administrado.
/system1/sp1	El procesador de servicio.
/system1/sol1	Destino de la comunicación en serie en la LAN.
/system1/sp1/account1 a /system1/sp1/account16	Las dieciséis cuentas locales de usuario de iDRAC6. account1 es la cuenta raíz.
/system1/sp1/enetport1	La dirección MAC del NIC del iDRAC6.
/system1/sp1/enetport1/lanendpt1 /ipendpt1	Los valores de la IP, la puerta de enlace y la máscara de red del iDRAC6.
/system1/sp1/enetport1/lanendpt1 /ipendpt1/dnsendpt1	La configuración del servidor DNS del iDRAC6.
/system1/sp1/group1 a /system1/sp1/group5	Los grupos de esquema estándar de Active Directory.
/system1/sp1/logs1	El destino de la recolecciones de registro.
/system1/sp1/logs1/record1	Una anotación individual del registro de sucesos de sistema en el sistema administrado.
/system1/sp1/logs1/records	El destino del SEL en el sistema administrado.
/system1/sp1/oemdell_racsecurity1	El almacenamiento para los parámetros que se usan para generar una solicitud de firma de certificado.
/system1/sp1/oemdell_ssl1	El estado de la solicitud de certificado de SSL.
/system1/sp1/oemdell_vmservice1	La configuración y estado de los medios virtuales.

Uso del verbo show

Para conocer más sobre un destino, utilice el verbo show. Este verbo muestra las propiedades del destino, subdestinos y una lista de los verbos de SM-CLP que se permiten en la ubicación.

Uso de la opción -display

La opción **show -display** permite limitar la salida del comando de manera que muestre una o más propiedades, destinos y verbos. Por ejemplo, para mostrar sólo las propiedades y destinos en la ubicación actual, use el comando siguiente:

```
show -d properties,targets /system1/sp1/account1
```

Para mostrar únicamente ciertas propiedades, indíquelas, según se muestra en el comando siguiente:

```
show -d properties=(userid,username) /system1/sp1/account1
```

Si sólo desea mostrar una propiedad, puede omitir los paréntesis.

Uso de la opción -level

La opción **show -level** ejecuta **show** en más niveles dentro del destino especificado. Por ejemplo, si desea consultar las propiedades **username** y **userid** de los destinos **account1** a **account16** bajo **/system1/sp1**, puede introducir el comando siguiente:

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

Para consultar todos los destinos y las propiedades en el espacio de direcciones, utilice la opción **-l all**, como se indica en el comando siguiente:

```
show -l all -d properties /
```

Uso de la opción -output

La opción **-output** especifica uno de cuatro formatos para la salida de los verbos de SM-CLP: **text**, **clpcsv**, **keyword** y **clpxml**.

El formato predeterminado es **text** y es el mensaje de salida más legible. El formato **clpcsv** es un formato de valores separados con comas que es apto para cargar un programa de hoja de cálculo. El formato **keyword** muestra la información a manera de lista de pares palabra_clave=valor, un par por línea. El formato **clpxml** es un documento XML que contiene el elemento XML **response**. DMTF creó especificaciones para los formatos **clpcsv** y **clpxml**, que se encuentran en el sitio web de DMTF en **www.dmtf.org**.

El ejemplo siguiente muestra cómo incluir el contenido del registro de sucesos del sistema en el mensaje de salida de XML:

```
show -l all -output format=clpxml /system1/sp1/logs1
```

Ejemplos de SM-CLP del iDRAC6

Los apartados siguientes contienen ejemplos para usar el SM-CLP para ejecutar las operaciones siguientes:

- Administración de la alimentación del servidor
- Administración del registro de sucesos del sistema
- Navegación del mapa de destino
- Mostrar las propiedades del sistema
- Establecimiento de la dirección IP, la máscara de subred y la dirección de puerta de enlace del iDRAC6

Para información sobre el uso de la interfaz SM-CLP de iDRAC6, consulte "Base de datos de propiedades SM-CLP del iDRAC6".

Administración de la alimentación del servidor

La tabla 14-4 contiene ejemplos de cómo usar el SM-CLP para realizar operaciones de administración de la alimentación del servidor en un servidor administrado.

Tabla 14-4. Operaciones de administración de la alimentación del servidor

Operación	Sintaxis
Inicio de sesión en el iDRAC6 por medio de la interfaz SSH	>ssh 192.168.0.120

	>login: root >password:
Apagar el servidor	->stop /system1 system1 has been stopped successfully
Encender el servidor a partir de un estado apagado	->start /system1 system1 has been started successfully
Reiniciar el servidor	->reset /system1 system1 has been reset successfully

Administración del registro de sucesos del sistema

La tabla 14-5 contiene ejemplos de cómo usar el SM-CLP para ejecutar operaciones relacionadas con el registro de sucesos del sistema en el sistema administrado.

Tabla 14-5. Operaciones de administración del registro de sucesos del sistema

Operación	Sintaxis
Ver el registro de sucesos del sistema	->show /system1/sp1/logs1 Targets: record1 record2 record3 record4 record5 Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5 Verbs: cd delete exit help show version
Ver la anotación del registro de sucesos del sistema	->show /system1/sp1/logs1/record4 ufip=/system1/sp1/logs1/log1/record4 Properties: Caption=Not defined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted ElementName=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI SEL CreationClassName=CIM_LogRecord RecordID=4 MessageTimeStamp=16:37:10,January 13,2007 Verbs: cd exit help show version
Borrar el registro de sucesos del sistema	->delete /system1/sp1/logs1 All records deleted successfully

Navegación del mapa de destino

La tabla 14-6 muestra ejemplos de cómo usar el verbo **cd** para navegar el mapa. En todos los ejemplos, se supone que el destino inicial predeterminado es /.

Tabla 14-6. Operaciones de navegación del mapa de destino

Operación	Sintaxis
Navegar hacia el sistema destino y reiniciar	->cd system1 ->reset

	NOTA: El destino predeterminado actual es **/**.

Navegar hacia el registro de sucesos del sistema de destino y mostrar las anotaciones del registro	`->cd system1`
	`->cd sp1`
	`->cd logs1`
	`->show`

	`->cd system1/sp1/logs1` `->show`
Mostrar el destino actual	`->cd .`
Subir un nivel	`->cd ..`
Salir del shell	`->exit`

Establecimiento de la dirección IP, la máscara de subred y la dirección de puerta de enlace del iDRAC6

El uso de SM-CLP para actualizar las propiedades de la red de iDRAC6 es un proceso de dos partes:

1. Establezca los nuevos valores de las propiedades de NIC en la ubicación **/ system1 / sp1 / enetport1 / lanendpt1 / ipendpt1:**
   - **oemdell_nicenable**: defina como **1** para activar el sistema de red del iDRAC6 y **0** para desactivarlo
   - **ipaddress**: la dirección IP
   - **subnetmask**: la máscara de subred
   - **oemdell_usedhcp**: defina como **1** para activar el uso de DHCP para establecer las propiedades **ipaddress** y **subnetmask**, **0** para establecer valores estáticos
2. Aplique los nuevos valores asignando un valor de **1** a la propiedad **committed**.

Siempre que la propiedad **commit** tenga el valor de 1, los valores actuales de las propiedades estarán activados. Cuando usted cambia alguna de las propiedades, la propiedad **commit** se restablece y recibe el valor de 0 para indicar que los valores no se han aplicado.

NOTA: La propiedad **commit** sólo afecta las propiedades en la ubicación de MAP **/system1 / sp1 / enetport1 / lanendpt1 / ipendpt1**. Todos los demás comandos de SM-CLP surten efecto inmediatamente.

NOTA: Si utiliza RACADM local para definir las propiedades de red del iDRAC6, los cambios surtirán efecto inmediatamente, pues RACADM local no depende de una conexión de red.

Cuando usted aplica los cambios, la nueva configuración de la red surte efecto, lo que hace que la sesión Telnet o SSH termine. Si incluye el paso de la opción commit, puede retrasar la terminación de la sesión hasta que haya terminado todos los comandos de SM-CLP.

La tabla 14-7 muestra ejemplos de cómo establecer las propiedades del iDRAC6 por medio de SM-CLP.

Tabla 14-7. Configuración de las propiedades de red del iDRAC6 con SM-CLP

Operación	**Sintaxis**
Desplazarse a la ubicación de las propiedades de la NIC del iDRAC6	`->cd /system1/sp1/enetport1/lanendpt1/ipendpt1`
Establecer la nueva dirección IP	`->set ipaddress=10.10.10.10`
Establecer la máscara de subred	`->set subnetmask=255.255.255.255`
Activar el indicador de DHCP	`->set oemdell_usedhcp=1`
Activar la tarjeta de interfaz de red	`->set oemdell_nicenable=1`
Aplicar los cambios	`->set committed=1`

Actualización del firmware del iDRAC6 por medio de SM-CLP

Para actualizar el firmware del iDRAC6 por medio de SM-CLP, se debe conocer el URI de TFTP para el paquete de actualización de Dell.

Siga estos pasos para actualizar el firmware por medio de SM-CLP:

1. Inicie sesión en el iDRAC6 por medio de Telnet o SSH.
2. Revise la versión del firmware actual con el comando siguiente:

   `version`

3. Introduzca el comando siguiente:

```
load -source tftp://<servidor_tftp>/<ruta_de_acceso_de_actualización> /system1/sp1
```

donde <*servidor_tftp*> es el nombre DNS o la dirección IP del servidor TFTP y <*ruta_de_acceso_de_actualización*> es la ruta de acceso al paquete de actualización en el servidor TFTP.

La sesión de Telnet o SSH se finalizará. Es posible que deba esperar varios minutos a que la actualización del firmware concluya.

4. Para verificar que se ha escrito el nuevo firmware, inicie una nueva sesión de Telnet o SSH y vuelva a introducir el comando de versión.

Regresar a la página de contenido

Regresar a la página de contenido

Instalación del sistema operativo por medio de iVMCLI

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

La utilidad de interfaz de línea de comandos de medios virtuales integrada (iVMCLI) es una interfaz de línea de comandos que ofrece las funciones de medios virtuales de la estación de administración al iDRAC6 en el sistema remoto. Por medio de la iVMCLI y los métodos con secuencias de comandos, usted puede instalar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información acerca de cómo integrar la utilidad iVMCLI en su red corporativa.

Antes de comenzar

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

Requisitos de los sistemas remotos

- El iDRAC6 se configura en cada sistema remoto.

Requisitos de red

Una área compartida de red debe tener los componentes siguientes:

- Los archivos de sistema operativo
- Los controladores necesarios
- Los archivos de imagen de inicio del sistema operativo

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

Creación de un archivo de imagen iniciable

Antes de instalar el archivo de imagen en los sistemas remotos, compruebe que el sistema compatible puede iniciar a partir del archivo. Para probar el archivo de imagen, transfiéralo a un sistema de prueba por medio de la interfaz de usuario web de iDRAC6 y luego reinicie el sistema.

Las secciones siguientes contienen información específica para la creación de archivos de imagen para los sistemas Linux y Windows.

Creación de un archivo de imagen para los sistemas Linux

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

Para ejecutar la utilidad, abra una ventana del símbolo del sistema e introduzca lo siguiente:

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

Por ejemplo:

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

Creación de un archivo de imagen para los sistemas Windows

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

Preparación para la instalación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que la estación de administración pueda acceder.
2. Copie los archivos de sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen iniciable preconfigurado para instalar el sistema operativo en los sistemas remotos, omita este paso.

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

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

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

   - Siga los procedimientos estándares de instalación basada en red.
   - Marque la imagen de instalación como "de sólo lectura" para garantizar que cada sistema de destino se inicie y se ejecute en el mismo procedimiento de instalación.
4. Realice uno de los procedimientos siguientes:
   - Integre **IPMItool** y la interfaz de línea de comandos de medios virtuales (iVMCLI) en la aplicación existente de instalación del sistema operativo. Use la secuencia de comandos de ejemplo **ivmdeploy** como guía para usar la utilidad.
   - Utilice la secuencia de comandos **ivmdeploy** existente para instalar el sistema operativo.

Instalación del sistema operativo

Use la utilidad iVMCLI y la secuencia de comandos **ivmdeploy** que se incluye con la utilidad para instalar el sistema operativo en los sistemas remotos.

Antes de comenzar, revise la secuencia de comandos **ivmdeploy** de ejemplo que se incluye con la utilidad iVMCLI. La secuencia de comandos muestra los pasos detallados que se necesitan para instalar el sistema operativo en los sistemas remotos de la red.

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

1. Haga una lista de las direcciones IP de iDRAC6 de los sistemas remotos que serán instalados en el archivo de texto **ip.txt**, una dirección IP por línea.
2. Inserte un CD o DVD iniciable de sistema operativo en la unidad correspondiente del cliente.
3. Ejecute **ivmdeploy** en la línea de comandos.

Para ejecutar la secuencia de comandos ivmdeploy, introduzca el siguiente comando en el símbolo del sistema:

```
ivmdeploy -r ip.txt -u <usuario_del_idrac> -p <contraseña_del_idrac> -c {<imagen_iso9660> | <ruta_de_acceso>}
```

donde:

- <*usuario_del_idrac*> es el nombre de usuario del iDRAC6, por ejemplo, **root**
- <*contraseña_del_idrac*> es la contraseña del usuario del iDRAC6, por ejemplo, **calvin**
- <*imagen_iso9660*> es la ruta de acceso de la imagen ISO9660 del CD o DVD de instalación del sistema operativo
- <*ruta_de_acceso*> es la ruta de acceso del dispositivo que contiene el CD o DVD de instalación del sistema operativo

La secuencia de comandos **ivmdeploy** pasa las opciones de línea de comandos a la utilidad **iVMCLI**. Consulte "Opciones de la línea de comandos" para obtener detalles sobre estas opciones. La secuencia de comandos procesa la opción **-r** de manera un poco distinta a la opción **iVMCLI -r**. Si el argumento de la opción **-r** es el nombre de un archivo existente, la secuencia de comandos leerá las direcciones IP de iDRAC6 del archivo especificado y ejecutará la utilidad **iVMCLI** una vez por cada línea. Si el argumento de la opción **-r** no es un nombre de archivo, deberá ser la dirección de un solo iDRAC6. En este caso, la opción **-r** funciona como se describe en la utilidad **iVMCLI**.

La secuencia de comandos ivmdeploy admite únicamente instalaciones a partir de un CD/DVD o de una imagen ISO9660 de CD/DVD. Si necesita instalar a partir de un disco flexible o de una imagen de disco flexible, puede modificar la secuencia de comandos para usar la opción **iVMCLI -f**.

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

La utilidad de interfaz de línea de comandos de medios virtuales (iVMCLI) es una interfaz de línea de comandos que se puede usar con secuencias de comandos y que suministra las funciones de medios virtuales de la estación de administración al iDRAC6.

La utilidad iVMCLI ofrece las siguientes funciones:

NOTA: Al hacer virtuales los archivos de imagen de sólo lectura, es posible que varias sesiones compartan el mismo medio de imagen. Al hacer virtuales las unidades físicas, sólo una sesión a la vez puede acceder a una unidad física determinada.

- Dispositivos de medios extraíbles o archivos de imagen que son congruentes con los complementos de medios virtuales
- Terminación automática cuando la opción para iniciar una vez del firmware de iDRAC6 está activada
- Comunicaciones seguras con el iDRAC6 por medio de la Capa de conexión segura (SSL)

Antes de que ejecutar la utilidad, compruebe que cuenta con privilegios de usuario de medios virtuales en el iDRAC6.

Si el sistema operativo admite los privilegios de administrador o una pertenencia a grupos o privilegio específico del sistema operativo, también deberá tener privilegios de administrador para poder ejecutar el comando iVMCLI.

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

Para sistemas Windows, se deben tener privilegios de usuario avanzado para poder ejecutar la utilidad iVMCLI.

En los sistemas Linux, se puede acceder a la utilidad iVMCLI sin tener privilegios de administrador por medio del comando **sudo**. Este comando brinda un medio centralizado para dar acceso sin privilegio de administrador y registra todos los comandos del usuario. Para agregar o editar usuarios en el grupo iVMCLI, el administrador usa el comando **visudo**. Los usuarios sin privilegios de administrador pueden agregar el comando **sudo** como prefijo a la línea de comandos de iVMCLI (o a la secuencia de comandos de iVMCLI) a fin de obtener acceso al iDRAC6 en el sistema remoto y ejecutar la utilidad.

Instalación de la utilidad iVMCLI

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

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

Además, el *DVD Dell Systems Management Tools and Documentation también* incluye **vmdeploy**: una secuencia de comandos de ejemplo que ilustra el uso de las utilidades iVMCLI y RACADM para instalar software en varios sistemas remotos.

NOTA: La secuencia de comandos **ivmdeploy** depende de otros archivos que están presentes en el directorio de la misma cuando se instala. Si desea usar la secuencia de comandos desde otro directorio, deberá copiar todos los archivos con ella.

Opciones de la línea de comandos

La interfaz iVMCLI es idéntica en los sistemas Windows y Linux. La utilidad usa opciones que son congruentes con las opciones de la utilidad RACADM. Por ejemplo, una opción para especificar la dirección IP de iDRAC6 requiere la misma sintaxis tanto en la utilidad RACADM como en la utilidad iVMCLI.

El formato del comando de iVMCLI es como se indica a continuación:

```
iVMCLI [parámetro] [opciones_de_shell_de_sistema_operativo]
```

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

Si el sistema remoto acepta los comandos y el iDRAC6 autoriza la conexión, el comando seguirá ejecutándose hasta que se presente cualquiera de los siguientes casos:

- La conexión de iVMCLI termina por algún motivo.
- El proceso se termina manualmente por medio de un control de sistema operativo. Por ejemplo, en Windows, se puede usar el Administrador de tareas para terminar el proceso.

Parámetros de iVMCLI

Dirección IP del iDRAC6.

```
-r <Dirección_IP_de_iDRAC>[:<puerto_SSL_de_iDRAC>]
```

Este parámetro proporciona la dirección IP del iDRAC6 y el puerto SSL, con los que la utilidad debe establecer una conexión de medios virtuales con el iDRAC6 de destino. Si introduce un nombre de DDNS o una dirección IP no válida, aparecerá un mensaje de error y el comando terminará.

donde <*dirección_IP_de_iDRAC6*> es una dirección IP válida y única, o bien, el nombre de Sistema dinámico de nombres de dominio (DDNS) de iDRAC6 (si se admite). Si se omite <*Puerto_SSL_de_iDRAC*>, se utilizará el puerto 443 (el puerto predeterminado). El puerto SSL opcional no es necesario a menos que se haya cambiado el puerto SSL predeterminado de iDRAC6.

Nombre de usuario del iDRAC6

```
-u <nombre_de_usuario_del_iDRAC>
```

Este parámetro proporciona el nombre de usuario de iDRAC6 que ejecutará los medios virtuales.

El <*nombre_de_usuario_de_iDRAC*> debe tener los atributos siguientes:

- Nombre de usuario válido
- Permiso de usuario de medios virtuales de iDRAC6

Si la autentificación de iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Contraseña de usuario del iDRAC6

`-p <contraseña_de_usuario_del_iDRAC>`

Este parámetro proporciona la contraseña para el usuario de iDRAC6 especificado.

Si la autenticación de iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Archivo de imagen o dispositivo de disco / disco flexible

`-f {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad válida (para sistemas Windows) o un nombre de archivo de dispositivo válido, incluyendo el número de partición del sistema de archivos montable, de ser aplicable (para sistemas Linux); y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo de imagen válido.

Este parámetro especifica el dispositivo o archivo que va a proporcionar el medio virtual de disco o disco flexible.

Por ejemplo, un archivo de imagen se especifica como:

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

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

Si el archivo no está protegido contra escritura, es posible que los medios virtuales escriban en el archivo de imagen. Configure el sistema operativo para proteger contra escritura una imagen de disco flexible que no desea que se sobrescriba.

Por ejemplo, un dispositivo se especifica como:

`-f a:\` (sistema Windows)

`-f /dev/sdb4 # 4ª partición en el dispositivo` /dev/sdb (sistema Linux)

Si el dispositivo tiene capacidad de protección contra escritura, utilice esta capacidad para garantizar que los medios virtuales no escribirán en el medio.

Omita este parámetro de la línea de comandos si no va a virtualizar discos flexibles. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Archivo de imagen o dispositivo de CD / DVD

`-c {<nombre_de_dispositivo> | <archivo_de_imagen>}`

donde <*nombre_de_dispositivo*> es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de archivo de dispositivo CD/DVD válido (sistemas Linux) y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo válido de imagen ISO-9660.

Este parámetro especifica el dispositivo o archivo que proporcionará el medio virtual de CD/DVD-ROM:

Por ejemplo, un archivo de imagen se especifica como:

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

`-c /tmp/mydvd.img` (sistemas Linux)

Por ejemplo, un dispositivo se especifica como:

`-c d:\` (sistemas Windows)

`-c /dev/cdrom` (sistemas Linux)

Omita este parámetro de la línea de comandos si no va a virtualizar discos CD/DVD. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Especifique al menos un tipo de medio (disco flexible o unidad de CD/DVD) con el comando, a menos que sólo se tengan opciones de interruptor. De lo contrario, aparecerá un mensaje de error y el comando terminará y producirá un error.

Mostrar la versión

`-v`

Este parámetro se usa para mostrar la versión de la utilidad iVMCLI. Si no se proporcionan otras opciones además de interruptores, el comando terminará sin mensajes de error.

Mostrar la ayuda

-h

Este parámetro muestra un resumen de los parámetros de la utilidad iVMCLI. Si no se proporcionan otras opciones además de conmutadores, el comando terminará sin errores.

Consulta del manual

-m

Este parámetro muestra una "página de manual" detallada de la utilidad iVMCLI, incluidas las descripciones de todas las opciones posibles.

Datos cifrados

-e

Cuando se incluya este parámetro en la línea de comandos, iVMCLI usará un canal cifrado con SSL para transferir datos entre la estación de administración y el iDRAC6 en el sistema remoto. Si este parámetro no se incluye en la línea de comandos, la transferencia de datos no se cifrará.

Opciones de shell de sistema operativo de iVMCLI

Las siguientes funciones del sistema operativo se pueden usar en la línea de comandos de iVMCLI:

- stderr/stdout redirection: desvía los mensajes de salida impresos hacia un archivo.

  Por ejemplo, al utilizar el carácter mayor que (>), seguido de un nombre del archivo, se sobrescribe el archivo especificado con el mensaje impreso de la utilidad iVMCLI.

  NOTA: La utilidad iVMCLI no lee la entrada estándar (**stdin**). En consecuencia, la redirección de **stdin** no es necesaria.

- Ejecución en segundo plano: de manera predeterminada, la utilidad iVMCLI se ejecuta en primer plano. Utilice las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en el segundo plano. Por ejemplo, en los sistemas operativos Linux, el carácter et (&) después del comando hace que el programa se genere como un nuevo proceso de segundo plano.

La última técnica es útil en programas de secuencias de comandos, ya que permite que la secuencia de comandos proceda después de que se inicia un nuevo proceso para el comando iVMCLI (de lo contrario, la secuencia de comandos se bloqueará hasta que el programa iVMCLI finalice). Cuando se inician varias instancias de iVMCLI de esta manera, y una o varias de las instancias de comando se finalizan manualmente, utilice las instalaciones específicas del sistema operativo para listar y finalizar procesos.

Códigos de retorno de iVMCLI

0 = Sin errores

1 = No se puede conectar

2 = Error de línea de comandos de iVMCLI

3 = Se cerró la conexión del firmware del RAC

Cuando se presentan errores, también se envían mensajes de texto en inglés a la salida estándar de errores.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la utilidad de configuración del iDRAC6

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Información general

La utilidad de configuración de iDRAC6 es un entorno de configuración de preinicio que permite visualizar y establecer parámetros para iDRAC6 y para el servidor administrado. Expresamente, usted puede:

- Ver los números de revisión del firmware del iDRAC6 y del firmware de la tarjeta primaria de plano posterior
- Configurar, activar o desactivar la red de área local (LAN) del iDRAC6
- Activar o desactivar la IPMI en la LAN
- Configurar los parámetros de LAN
- Activar, desactivar o cancelar System Services
- Conectar o desconectar los dispositivos de medios virtuales
- Cambiar el nombre de usuario administrativo y la contraseña
- Restablecer la configuración predeterminada de fábrica del iDRAC6
- Ver o borrar los mensajes del registro de sucesos del sistema (SEL)

Las tareas que puede realizar con la utilidad de configuración del iDRAC6 también pueden realizarse mediante otras utilidades que se incluyen con el iDRAC6 o el software OpenManage del Dell, incluida la interfaz basada en web, la interfaz de línea de comandos de SM-CLP, la interfaz de línea de comandos de RACADM local y, en el caso de la configuración de red básica, en la pantalla LCD del iDRAC6 durante la configuración inicial del iDRAC6.

Inicio de la utilidad de configuración del iDRAC6

Se debe usar una consola conectada al KVM de iDRAC6 para tener acceso a la utilidad de configuración del iDRAC6 al inicio o después de restablecer la configuración predeterminada del iDRAC6.

1. En el teclado conectado a la consola KVM del iDRAC6, presione <Impr Pant> para mostrar el menú de **OSCAR (On Screen Configuration and Reporting)** del KVM de iDRAC6. Use las teclas de <Flecha ascendente> y <Flecha descendente> para resaltar la ranura que contiene el servidor y después presione <Entrar>.
2. Encienda o reinicie el servidor con el botón de encendido que se encuentra en el frente del servidor.
3. Cuando aparezca el mensaje Press <Ctrl-E> for Remote Access Setup within 5 sec (Presione <Ctrl-E> para la configuración de acceso remoto dentro de 5 segundos)..., presione inmediatamente <Ctrl><E>. Aparecerá la utilidad de configuración del iDRAC6.

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

Las dos primeras líneas de la utilidad de configuración ofrecen información sobre el firmware del iDRAC6 y las revisiones del firmware de la tarjeta primaria de plano posterior. Los niveles de revisión pueden ser útiles para determinar si una actualización de firmware es necesaria.

El firmware del iDRAC6 es la parte del firmware que se encarga de las interfaces externas, por ejemplo, la interfaz basada en web, SM-CLP y las interfaces web. El firmware de la tarjeta primaria de plano posterior es la parte del firmware que se conecta y supervisa el entorno de hardware del servidor.

Uso de la utilidad de configuración del iDRAC6

Bajo los mensajes de revisión de firmware, el resto de la utilidad de configuración del iDRAC6 es un menú de opciones a las que puede tener acceso por medio de las teclas de flecha ascendente y flecha descendente.

- Si una opción del menú conduce a un submenú o a un campo de texto editable, presione <Entrar> para acceder a la opción y <Esc> para salir de la misma después de terminar de configurarla.
- Si un elemento tiene valores que se pueden seleccionar, como Sí/No o Activado/Desactivado, presione la flecha hacia la izquierda, la flecha hacia la derecha o la barra espaciadora para elegir un valor.
- Si un elemento no se puede editar, aparecerá en azul. Algunos elementos se pueden editar en función de otras selecciones que usted haga.
- La línea en la parte inferior de la pantalla muestra instrucciones relacionadas con el elemento actual. Puede presionar <F1> para mostrar la ayuda del elemento actual.

- Cuando haya terminado de usar la utilidad de configuración del iDRAC6, presione <Esc> para consultar el menú de salida, donde podrá elegir si desea guardar o descartar los cambios o volver a la utilidad.

Las secciones siguientes describen las opciones del menú de la utilidad de configuración del iDRAC6.

LAN de iDRAC6

Use la flecha hacia la izquierda, la flecha hacia la derecha y la barra espaciadora para seleccionar entre **Activado** y **Desactivado**.

La LAN del iDRAC6 está desactivada en la configuración predeterminada. Es necesario activar la LAN para permitir el uso de los servicios del iDRAC6 tales como la interfaz basada en web, el acceso Telnet/SSH a la interfaz de línea de comandos de SM-CLP, la redirección de consola y los medios virtuales.

Si elige desactivar la LAN, aparecerá la siguiente advertencia:

```
iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.
(La interfaz del iDRAC fuera de banda se desactivará si el canal de LAN está desactivado.)
```

El mensaje le informa que, además de los servicios a los que tiene acceso a través de la conexión directa del iDRAC6, HTTP, HTTPS, Telnet o los puertos SSH, el tráfico de red de administración fuera de banda, por ejemplo, los mensajes de IPMI que se envían al iDRAC6 desde una estación de administración, no se recibe cuando la LAN está desactivada. La interfaz RACADM local permanece disponible y se puede usar para reconfigurar la LAN de iDRAC6.

```
Presione cualquier tecla para quitar el mensaje y continuar.
```

IPMI en la LAN

Presione la flecha hacia la izquierda, la flecha hacia la derecha y la barra espaciadora para seleccionar entre **Activada** y **Desactivada**. Cuando se seleccione **Desactivada**, el iDRAC6 no aceptará mensajes IPMI que lleguen por medio de la interfaz de LAN.

Si elige **Desactivada**, aparecerá la siguiente advertencia:

```
iDRAC Out-of-Band interface will be disabled if IPMI Over LAN is OFF.
(La interfaz del iDRAC fuera de banda se desactivará si el canal de LAN está desactivado.)
```

Presione cualquier tecla para quitar el mensaje y continuar. Para ver una explicación del mensaje, consulte "LAN de iDRAC6".

Parámetros de LAN

Presione <Entrar> para mostrar el submenú de parámetros de la LAN. Cuando haya terminado de configurar los parámetros de la LAN, presione <Esc> para volver al menú anterior.

Tabla 16-1. Parámetros de LAN

Elemento	Descripción
Clave de cifrado de RMCP+	Presione <Entrar> para modificar el valor, <Esc> cuando haya terminado. La clave de cifrado de RMCP+ es una cadena hexadecimal de 40 caracteres (caracteres 0-9, a-f y A-F). RMCP+ es una extensión de IPMI que agrega la autentificación y el cifrado a IPMI. El valor predeterminado es una cadena de 40 ceros.
Fuente de dirección IP	Seleccione entre **DHCP** y **Estática**. Cuando se selecciona DHCP, los campos **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se obtienen de un servidor DHCP. Si no se encuentra ningún servidor DHCP en la red, los campos tomarán valores de ceros. Cuando se selecciona **Estática**, las opciones **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se pueden editar**.**
Dirección IP de Ethernet	Si la opción **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC. El valor predeterminado es **192.168.0.120** más el número de la ranura que contiene el servidor.
MAC Address	Ésta es la dirección MAC no editable de la interfaz de red del iDRAC6.
Máscara de subred	Si la **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección de máscara de subred que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la máscara de subred para el iDRAC. El valor predeterminado es **255.255.255.0**.
Puerta de enlace predeterminada	Si la **Fuente de la dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si la **Fuente de la dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada. El valor predeterminado es **192.168.0.1**.
Alerta de LAN activada	Seleccione **Activada** para activar la alerta de captura de sucesos de plataforma (PET) de LAN.
Anotación de política de alerta 1	Seleccione Activar o Desactivar para activar el primer destino de alerta.

Destino de alerta 1	Introduzca la dirección IP a la que se enviarán las alertas de captura de sucesos de plataforma de la LAN.
Cadena de nombre del host	Presione <Entrar> para editarla. Introduzca el nombre del host para las alertas de captura de sucesos de plataforma.
Servidores DNS de DHCP	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidor DNS. Seleccione **Desactivado** para especificar las direcciones de servidor DNS a continuación.
Servidor DNS 1	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del primer servidor DNS.
Servidor DNS 2	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del segundo servidor DNS.
Registrar el nombre del iDRAC	Seleccione **Activado** para registrar el nombre del iDRAC6 en el servicio DNS. Seleccione **Desactivado** si no desea que los usuarios puedan encontrar el nombre del iDRAC6 en el DNS.
Nombre del iDRAC	Si **Registrar el nombre del iDRAC** se encuentra **Activado**, presione <Entrar> para modificar el campo de texto **Nombre actual del iDRAC de DNS**. Oprima <Entrar> cuando haya terminado de modificar el nombre del iDRAC6. Oprima <Esc> para volver al menú anterior. El nombre del iDRAC6 debe ser un nombre de host DNS válido.
Nombre de dominio de DHCP	Seleccione **Activado** si desea obtener el nombre de dominio de un servicio DHCP de la red. Seleccione **Desactivado** si desea especificar el nombre de dominio.
Nombre de dominio	Si **Nombre de dominio de DHCP** esta **Desactivado**, presione <Entrar> para modificar el campo de texto **Nombre de dominio actual**. Presione <Entrar> cuando haya terminado de modificarlo. Oprima <Esc> para volver al menú anterior. El nombre de dominio debe ser un dominio DNS válido, por ejemplo, `miempresa.com`.

Configuración de medios virtuales

Medios virtuales

Use la flecha hacia la izquierda y la flecha hacia la derecha para seleccionar **Conectado** o **Desconectado**.

- Si se selecciona **Conectado**, los dispositivos de medios virtuales se conectan al bus USB y están listos para su uso durante las sesiones de **Redirección de consola**.
- Si selecciona **Desconectado**, los usuarios no podrán acceder a los dispositivos de medios virtuales durante las sesiones de **Redirección de consola**.

NOTA: Para usar una unidad flash USB con la función de Medios virtuales, debe establecer la opción **Tipo de emulación de unidad flash USB** como **Disco duro** en la utilidad de configuración del BIOS. Se accede a la utilidad de configuración del BIOS al presionar <F2> durante el arranque del servidor. Si el **Tipo de emulación de la unidad flash USB** se establece como **Automático**, la unidad flash aparecerá como unidad de disco flexible en el sistema.

Unidad flash virtual

Use la flecha hacia la izquierda y la flecha hacia la derecha para seleccionar **Activado** o **Desactivado**.

- **Activado**/**desactivado** hace que todos los dispositivos virtuales del bus USB se **desconecten** y **conecten**.
- **Desactivado** hace que la memoria virtual flash se elimine y deje de estar disponible para uso.

NOTA: Este campo puede ser de sólo lectura si en la ranura para tarjetas AMEA no hay una tarjeta SD con un tamaño superior a 256 MB.

NOTA: Se necesita una tarjeta multimedia vFlash marca Dell para la partición flash virtual.

Configuración de los servicios del sistema

System Services

Use la flecha hacia la izquierda y la flecha hacia la derecha para seleccionar **Activado** o **Desactivado**. En caso de estar activados, algunas funciones de iDRAC6 se pueden configurar a través de Unified Server Configuration (USC). Para obtener más información, consulte la *Guía del usuario de Unified Server Configurator,* disponible en el sitio web de asistencia de Dell: **support.dell.com**.

NOTA: Si modifica esta opción, el servidor se reiniciará cuando presione **Guardar** y **Salir** para aplicar la nueva configuración.

Cancelación de System Services

Use la flecha hacia la izquierda y la flecha hacia la derecha para seleccionar **Sí** o **No**.

Al seleccionar **Sí**, se cierran todas las sesiones de Unified Server Configurator y el servidor se reinicia al presionar **Guardar** y **Salir** para aplicar la nueva configuración.

Configuración de usuario de la LAN

El usuario de la LAN es la cuenta de administrador del iDRAC6, que tiene el nombre predeterminado **root**. Presione <Entrar> para mostrar el submenú de configuración de usuario de la LAN. Cuando haya terminado de configurar el usuario de la LAN, presione <Esc> para volver al menú anterior.

Tabla 16-2. Pantalla de configuración de usuarios de la LAN

Elemento	Descripción
Acceso de cuenta	Seleccione **Activado** para activar la cuenta de administrador. Seleccione **Desactivado** para desactivar la cuenta de administrador.
Privilegio de cuenta	Seleccione **Admin**, **Usuario**, **Operador** o **Sin acceso**.
Nombre de usuario de la cuenta	Presione <Entrar> para modificar el nombre de usuario y presione <Esc> cuando haya terminado. El nombre de usuario predeterminado es **root**.
Introducir la contraseña	Introduzca la nueva contraseña para la cuenta de administrador. Los caracteres no aparecerán en la pantalla cuando usted los introduzca.
Confirmar la contraseña	Introduzca nuevamente la nueva contraseña para la cuenta de administrador. Si los caracteres que introduce no coinciden con los caracteres que introdujo en el campo **Introducir la contraseña**, aparecerá un mensaje y usted deberá introducir nuevamente la contraseña.

Restablecer valores predeterminados

Use la opción de menú **Restablecer valores predeterminados** para restablecer todos los valores predeterminados de fábrica de las opciones de configuración del iDRAC6. Esto puede ser necesario, por ejemplo, cuando usted ha olvidado la contraseña del usuario administrativo o si desea volver a configurar el iDRAC6 a partir de los valores predeterminados.

NOTA: En la configuración predeterminada, el sistema de red del iDRAC6 está desactivado. Usted no podrá reconfigurar el iDRAC6 por medio de la red hasta que haya activado la red del iDRAC6 en la utilidad de configuración del iDRAC6.

Presione <Entrar> para seleccionar el elemento. Aparecerá el siguiente mensaje de advertencia:

```
Resetting to factory defaults will restore remote Non-

Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >

(Si restablece los valores predeterminados de fábrica restaurará la configuración no volátil de usuario remoto. ¿Continuar?

< NO (Cancelar) >

< SÍ (Continuar) > )
```

Para restablecer los valores predeterminados de iDRAC6, seleccione **SÍ** y presione <Entrar>.

Menú del registro de sucesos del sistema

El menú **Registro de sucesos del sistema** permite ver y borrar los mensajes del Registro de sucesos del sistema (SEL). Presione <Entrar> para mostrar el **Menú del registro de sucesos del sistema**. El sistema cuenta las anotaciones del registro y después muestra el número total de anotaciones y el mensaje más reciente. El registro de sucesos del sistema retiene un máximo de 512 mensajes.

Para ver los mensajes del registro de sucesos del sistema, seleccione **Ver registro de sucesos del sistema** y presione <Entrar>. Para desplazarse:

- Use la flecha hacia la izquierda para retroceder al mensaje anterior (más antiguo) y la flecha hacia la derecha para avanzar al mensaje siguiente (más reciente).
- Introduzca un número de registro específico para ir directamente al registro.

Presione <Esc> para salir del Registro de sucesos del sistema.

NOTA: Sólo puede borrar el registro de sucesos del sistema en la utilidad de configuración del iDRAC6 o en la interfaz basada en web del iDRAC6.

Para borrar el registro de sucesos del sistema, seleccione **Borrar el registro de sucesos del sistema** y presione <Entrar>.

Cuando haya terminado con el menú de registro de sucesos del sistema, presione <Esc> para volver al menú anterior.

Salida de la utilidad de configuración del iDRAC6

Cuando haya terminado de hacer cambios en la configuración del iDRAC6, presione la tecla <Esc> para mostrar el menú de salida.

Seleccione **Guardar cambios y salir** y presione <Entrar> para retener los cambios.

Seleccione **Descartar cambios y salir** y presione <Entrar> para ignorar los cambios que ha realizado

Seleccione **Regresar a la configuración** y presione <Entrar> para volver a la utilidad de configuración del iDRAC6.

Regresar a la página de contenido

Regresar a la página de contenido

Recuperación y solución de problemas del servidor administrado

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Esta sección explica cómo realizar tareas relacionadas con el diagnóstico y la solución de problemas de un servidor administrado remoto por medio de las utilidades de iDRAC6. Contiene los apartados siguientes:

- Indicadores de problemas: ayuda a encontrar mensajes y otros indicadores del sistema que pueden conducir a un diagnóstico del problema
- Herramientas para solución de problemas: describe las herramientas de iDRAC6 que se pueden usar para solucionar problemas del sistema
- Solución de problemas y preguntas frecuentes: respuestas a situaciones típicas que usted puede encontrar

---

La seguridad es lo primero; para usted y su sistema

Para realizar ciertos procedimientos de esta sección, se debe trabajar con el chasis, el servidor PowerEdge u otros módulos de hardware. No intente reparar el hardware del sistema salvo según se explica en esta guía y en otra parte en la documentación del sistema.

△ **PRECAUCIÓN: Muchas de las reparaciones deben realizarlas únicamente los técnicos de servicio autorizados. Usted sólo deberá aplicar las soluciones de problemas y reparaciones simples que se autoricen en la documentación del producto o según lo indique el equipo de asistencia técnica por teléfono o en línea. La garantía no cubre los daños ocasionados por reparaciones que Dell no haya autorizado. Lea y siga las instrucciones de seguridad que se entregan con el producto.**

Indicadores de problemas

Esta sección describe indicadores que sugieren que puede haber un problema en el sistema.

Indicadores LED

Los indicadores LED del chasis o de los componentes instalados en el chasis son generalmente los primeros indicadores de problemas en el sistema. Los siguientes componentes y módulos tienen indicadores LED de estado:

- Pantalla LCD del chasis
- Servidores
- Ventiladores
- CMC
- Módulos de E/S
- Fuentes de alimentación

El indicador LED de la pantalla LCD del chasis resume el estado de todos los componentes del sistema. Un LED de color azul indica que no se han detectado condiciones de falla en el sistema. Si el LED parpadea en color ámbar, indica que se han detectado una o más condiciones de falla.

Si la pantalla LCD del chasis tiene un LED que parpadea en color ámbar, se puede usar el menú de la pantalla LCD para localizar el componente que tiene la falla. Consulte la *Guía del usuario del firmware del CMC Dell* para ayuda sobre la utilización de la pantalla LCD.

La tabla 17-1 describe el significado del comportamiento del indicador LED del servidor PowerEdge:

Tabla 17-1. Indicadores LED del servidor

Indicador LED	Significado
verde continuo	El servidor está encendido. La ausencia del indicador LED en color verde significa que el servidor no está encendido.
azul continuo	El iDRAC6 presenta una condición satisfactoria.
parpadeo en color ámbar	El iDRAC6 ha detectado una condición de falla o es posible que esté en proceso de actualizar el firmware.
parpadeo en color azul	Un usuario ha activado la identificación de localizador de este servidor.

Indicadores de problemas del hardware

Los indicadores de que un módulo tiene un problema de hardware incluyen los siguientes:

- Falla de encendido
- Ventiladores ruidosos
- Pérdida de conectividad de red
- Alertas de los sensores de supervisión de la batería, temperatura, voltaje o alimentación
- Fallas de disco duro
- Falla de medios USB
- Daños físicos provocados por caídas, agua u otros agentes externos

Cuando se presentan estos tipos de problemas, puede intentar corregir el problema con estas estrategias:

- Reasiente el módulo y reinícielo
- Inserte el módulo en otro compartimiento del chasis
- Sustituya los discos duros o memorias USB
- Vuelva a conectar o reemplace los cables de alimentación y de red

Si estos pasos no corrigen el problema, consulte el *Manual del propietario del hardware* para obtener información específica de solución de problemas del dispositivo de hardware.

Otros indicadores de problemas

Tabla 17-2. Indicadores de problemas

Buscar:	**Acción:**
Mensajes de alerta procedentes del software de administración de sistemas	Consulte la documentación del software de administración de sistemas.
Mensajes en el registro de sucesos del sistema	Consulte "Consulta del registro de sucesos del sistema (SEL)".
Mensajes en los códigos POST de inicio	Consulte "Consulta de los códigos POST".
Mensajes en la pantalla de último bloqueo	Consulte "Visualización de la pantalla de último bloqueo del sistema".
Mensajes de alerta en la pantalla de estado del servidor de la LCD	Consulte "Consulta de la pantalla de estado del sistema en busca de mensajes de error".
Mensajes en el registro del iDRAC6	Consulte "Visualización del registrodel iDRAC6".

Herramientas para solución de problemas

Esta sección describe las utilidades del iDRAC6 que se pueden usar para diagnosticar problemas del sistema, sobre todo cuando usted trata de solucionar problemas de manera remota.

- Consulta de la condición del sistema
- Consulta del registro de sucesos del sistema en busca de mensajes de error
- Consulta de los códigos POST
- Visualización de la pantalla de último bloqueo
- Consulta de la pantalla de estado del servidor en la pantalla LCD en busca de mensajes de error
- Visualización del registro del iDRAC6
- Acceso a la información del sistema
- Identificación del servidor administrado en el chasis
- Uso de la consola de diagnósticos
- Administración de alimentación en un sistema remoto

Consulta de la condición del sistema

Al iniciar sesión en la interfaz web del iDRAC6, la primera pantalla que aparece describe la condición de los componentes del sistema. La tabla 17-3 describe el significado de los indicadores de condición del sistema.

Tabla 17-3. Indicadores de condición del sistema

Indicador	Descripción
	Una marca de verificación verde indica una condición de estado sana (normal).
	Un triángulo amarillo que contiene un signo de admiración indica una condición de estado de advertencia (no crítica).
	Una X roja indica una condición de estado crítica (falla).
	Un icono con un signo de interrogación indica que se desconoce el estado.

Haga clic en cualquier componente en la pantalla **Condición** para ver la información sobre el componente. Se muestran las lecturas de sensores de baterías, temperaturas, voltajes y supervisión de alimentación, lo que ayuda a diagnosticar algunos tipos de problemas. Las pantallas de información del iDRAC6 y el CMC muestran información útil sobre el estado actual y la configuración.

Consulta del registro de sucesos del sistema (SEL)

La pantalla **Registro SEL** muestra los mensajes de los sucesos que ocurren en el servidor administrado.

Para ver el **Registro de sucesos del sistema**, realice los pasos a continuación:

1. Haga clic en **Sistema** y después haga clic en la ficha **Registros**.
2. Haga clic en **Registro de sucesos del sistema** para mostrar la pantalla **Registro de sucesos del sistema**.

   La pantalla **Registro de sucesos del sistema** muestra un indicador de condición del sistema (consulte la tabla 17-3), la fecha y hora, y una descripción del suceso.
3. Haga clic en el botón **Registro de sucesos del sistema** correspondiente para continuar (consulte la tabla 17-4).

Tabla 17-4. Botones del registro de sucesos del sistema

Botón	Acción
Imprimir	Imprime el **registro de sucesos del sistema en el orden en que aparece en la ventana.**
Borrar registro	Borra el **registro de sucesos del sistema**. **NOTA:** El botón **Borrar registro** sólo aparece si tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **registro de sucesos del sistema** en el directorio de su elección. **NOTA:** Si va a usar Internet Explorer y encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft® en support.microsoft.com.
Actualizar	Vuelve a cargar la pantalla **Registro de sucesos del sistema**.

Consulta de los códigos POST

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

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

Para ver los códigos POST, realice los pasos siguientes:

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

   La pantalla **Códigos POST** muestra un indicador de condición del sistema (consulte la tabla 17-3), un código hexadecimal y una descripción del código.
2. Haga clic en el botón **Código POST** correspondiente para continuar (consulte la tabla 17-5).

Tabla 17-5. Botones de códigos POST

Botón	Acción
Imprimir	Imprime la pantalla **Códigos POST.**
Actualizar	Vuelve a cargar la pantalla **Códigos POST**.

Visualización de la pantalla de último bloqueo del sistema

NOTA: La función de pantalla de último bloqueo se debe configurar en Server Administrator y en la interfaz web del iDRAC6. Consulte "Configuración del servidor administrado para capturar la pantalla de último bloqueo" para obtener instrucciones sobre cómo configurar esta función.

La **Pantalla de último bloqueo** muestra la pantalla del bloqueo más reciente, que incluye información sobre los sucesos que ocurrieron antes de que el sistema se bloqueara. La imagen del último bloqueo del sistema se guarda en la memoria permanente del iDRAC6 y se puede acceder a ella de manera remota.

Para ver la **Pantalla de último bloqueo**, realice los pasos a continuación:

- Haga clic en la ficha **Sistema**, en la ficha **Registros** y luego haga clic en **Último bloqueo**.

La **Pantalla de último bloqueo** tiene los botones que se muestran en la tabla 17-6:

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

Tabla 17-6. Botones de la Pantalla de último bloqueo

Botón	Acción
Imprimir	Imprime la **Pantalla de último bloqueo**.
Guardar	Abre una ventana emergente que permite guardar la **pantalla de último bloqueo** en el directorio de su elección.
Eliminar	Elimina la **Pantalla de último bloqueo**.
Actualizar	Vuelve a cargar la **Pantalla de último bloqueo**.

NOTA: Debido a fluctuaciones en el temporizador de la recuperación automática, es posible que la **Pantalla de último bloqueo** no pueda capturarse cuando el temporizador de restablecimiento del sistema tenga un valor demasiado alto. El valor predeterminado es de 480 segundos. Utilice Server Administrator o IT Assistant para definir el temporizador de restablecimiento del sistema como 60 segundos y para asegurarse de que la **Pantalla de último bloqueo** funcione correctamente. Para obtener información adicional, consulte "Configuración del servidor administrado para capturar la pantalla de último bloqueo".

Consulta de las secuencias de inicio más recientes

Si experimenta problemas de inicio, puede ver la actividad de pantalla de lo que ha sucedido durante las últimas tres secuencias de inicio de la pantalla **Captura de inicio**. La reproducción de las pantallas de inicio ocurre a una velocidad de 1 marco por segundo. La tabla 17-7 presenta una lista de las acciones de control disponibles.

NOTA: Debe disponer de privilegios de administrador para ver la reproducción de las secuencias de Captura de inicio.

Tabla 17-7. Opciones de Captura de inicio

Botón/Opción	Descripción
Selecciona la secuencia de inicio	Permite seleccionar la secuencia de inicio para cargar y reproducir. - Captura de inicio 1: carga la secuencia de inicio más reciente. - Captura de inicio 2: carga la secuencia de inicio (segunda más reciente) que ocurrió antes de la Captura de inicio 1. - Captura de inicio 3: carga la secuencia de inicio (tercera más reciente) que ocurrió antes de la Captura de inicio 2.
Guardar como	Crea un archivo .zip comprimido que contiene todas las imágenes de captura de inicio de la secuencia actual. El usuario debe disponer de privilegios de administración para realizar esta acción.
Pantalla anterior	Lo lleva a la pantalla anterior, de existir, en la consola de reproducción.
Reproducir	Inicia la reproducción de la pantalla actual en la consola de reproducción.
Pausa	Interrumpe la reproducción en la pantalla actual que se está mostrando en la consola de reproducción.
Stop	Detiene la reproducción de pantalla y carga la primera pantalla de esa secuencia de inicio.
Próxima pantalla	Lo lleva a la pantalla siguiente, de existir, en la consola de reproducción.
Imprimir	Imprime la imagen de Captura de inicio que aparece en la pantalla.
Actualizar	Vuelve a cargar la pantalla de Captura de inicio.

Consulta de la pantalla de estado del sistema en busca de mensajes de error

Cuando un indicador LED parpadea en color ámbar y un servidor específico tiene un error, la pantalla de estado del servidor principal en la pantalla LCD resaltará el servidor afectado con un color naranja. Use los botones de navegación de la pantalla LCD para resaltar el servidor afectado y después haga clic en el botón central. Los mensajes de error y advertencia aparecerán en la segunda línea. La tabla siguiente muestra una lista de todos los mensajes de error y la gravedad de los mismos.

Tabla 17-8. Pantalla de estado del servidor

Gravedad	Mensaje	Causa
Advertencia	System Board Ambient Temp: Temperature sensor for System Board, warning event (Temperatura ambiental de la placa del sistema: sensor de temperatura de la placa del sistema, suceso de advertencia)	La temperatura ambiental del servidor superó el umbral de advertencia
Crítico	System Board Ambient Temp: Temperature sensor for System Board, failure event (Temperatura ambiental de la placa del sistema: sensor de temperatura de la placa del sistema, suceso de falla)	La temperatura ambiental del servidor superó el umbral de falla
Crítico	System Board CMOS Battery: Battery sensor for System Board, failed was asserted (Batería CMOS de la placa del sistema: sensor de la batería de la placa del sistema, se confirmó una falla)	No hay batería CMOS o no tiene carga
Advertencia	System Board System Level: Current sensor for System Board, warning event (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	System Board System Level: Current sensor for System Board, failure event (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<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU<número> <nombre del sensor de voltaje>: sensor de voltaje de la CPU<número>, se confirmó el estado declarado)	Voltaje fuera de rango
Crítico	System Board <voltage sensor name>: Voltage sensor for System Board, state asserted was asserted (<Nombre del sensor de voltaje> de la placa del sistema: sensor de voltaje de la placa del sistema, se confirmó el estado declarado)	Voltaje fuera de rango
Crítico	CPU<number> <voltage sensor name>: Voltage sensor for CPU<number>, state asserted was asserted (CPU<número> <nombre del sensor de voltaje>: sensor de voltaje de la CPU<número>, se confirmó el estado declarado)	Voltaje fuera de rango
Crítico	CPU<number> Status: Processor sensor for CPU<number, IERR was asserted (Estado de la CPU<número>: sensor de procesador de la CPU<número>, se confirmó IERR)	Falla de la CPU
Crítico	CPU<number> Status: Processor sensor for CPU<number>, thermal tripped was asserted (Estado de la CPU<número>: sensor de procesador de la CPU<número>, se confirmó un disparo térmico)	La CPU se sobrecalentó
Crítico	CPU<number> Status: Processor sensor for CPU<number, configuration error was asserted (Estado de la CPU<número>: sensor de procesador de la CPU<número>, se confirmó un error de configuración)	Tipo incorrecto de procesador o instalación en el lugar erróneo
Crítico	CPU<number> Status: Processor sensor for CPU<number>, presence was deasserted (Estado de la CPU<número>: sensor de procesador de la CPU<número>, no se confirmó la presencia)	La CPU requerida no se encuentra o no está presente
Crítico	System Board Video Riser: Module sensor for System Board, device removed was asserted (Tarjeta vertical de vídeo de la placa del sistema: sensor de módulo de la placa del sistema, se confirmó el retiro del dispositivo)	Se retiró el módulo requerido
Crítico	Mezz B<slot number> Status: Add-in Card sensor for Mezz B<slot number>, install error was asserted (Estado de la tarjeta intermediaria B<número de ranura>: sensor de tarjeta de complemento para la tarjeta intermediaria B<número de ranura>, se confirmó un error de instalación)	Se instaló una tarjeta intermediaria incorrecta para la red Fabric de E/S
Crítico	Mezz C<slot number> Status: Add-in Card sensor for Mezz C<slot number>, install error was asserted (Estado de la tarjeta intermediaria C<número de ranura>: sensor de tarjeta de complemento para la tarjeta intermediaria C<número de ranura>, se confirmó un error de instalación)	Se instaló una tarjeta intermediaria incorrecta para la red Fabric de E/S
Crítico	Backplane Drive <number>: Drive Slot sensor for Backplane, drive removed (Unidad de plano posterior <número>: sensor de ranura de unidad del plano posterior, se retiró la unidad)	Se retiró la unidad de almacenamiento
Crítico	Backplane Drive <number>: Drive Slot sensor for Backplane, drive fault was asserted (Unidad de plano posterior <número>: sensor de ranura de unidad del plano posterior, se confirmó una falla de la unidad)	Falló la unidad de almacenamiento
Crítico	System Board PFault Fail Safe: Voltage sensor for System Board, state asserted was asserted (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	System Board OS Watchdog: Watchdog sensor for System Board, timer expired was asserted (Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó que el temporizador ha expirado)	El temporizador de la vigilancia de iDRAC6 expiró y no se estableció ninguna acción
Crítico	System Board OS Watchdog: Watchdog sensor for System Board,	La vigilancia de iDRAC6 detectó que el sistema se ha bloqueado (el

	reboot was asserted (Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó un reinicio)	temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de reiniciar
Crítico	System Board OS Watchdog: Watchdog sensor for System Board, power off was asserted (Vigilancia del sistema operativo de la placa del sistema: sensor de vigilancia de la placa del sistema, se confirmó el apagado)	La vigilancia de iDRAC6 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	System Board OS Watchdog: Watchdog sensor for System Board, power cycle was asserted (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 iDRAC6 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	System Board SEL: Event Log sensor for System Board, log full was asserted (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	ECC Corr Err: Memory sensor, correctable ECC (<DIMM Location>) was asserted (Error corregible de ECC: sensor de memoria, se confirmó un ECC corregible (<ubicación del DIMM>))	Los errores ECC corregibles alcanzaron una frecuencia crítica
Crítico	ECC Uncorr Err: Memory sensor, uncorrectable ECC (<DIMM Location>) was asserted (Error no corregible ECC: Sensor de memoria, se confirmó el ECC no corregible (<Ubicación del módulo DIMM>))	Se detectó un error ECC incorregible
Crítico	I/O Channel Chk: Critical Event sensor, I/O channel check NMI was asserted (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	PCI Parity Err: Critical Event sensor, PCI PERR was asserted (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	PCI System Err: Critical Event sensor, PCI SERR (<Slot number or PCI Device ID>) was asserted (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	SBE Log Disabled: Event Log sensor, correctable memory error logging disabled was asserted (Registro SBE desactivado: sensor de registro de sucesos, se confirmó la desactivación del registro de errores corregibles de memoria)	El registro de errores de un solo bit se desactiva cuando se registran demasiados SBE (errores de un solo bit)
Crítico	Logging Disabled: Event Log sensor, all event logging disabled was asserted (Desactivación de registro: sensor del registro de sucesos, se confirmó la desactivación de todo registro de sucesos)	Se desactivó todo registro de errores
No recuperable	CPU Protocol Err: Processor sensor, transition to non-recoverable was asserted (Error de protocolo de CPU: sensor de procesador, se confirmó la transición a estado no recuperable)	El protocolo del procesador ingresó en un estado no recuperable
No recuperable	CPU Bus PERR: Processor sensor, transition to non-recoverable was asserted (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	CPU Init Err: Processor sensor, transition to non-recoverable was asserted (Error de inicialización de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable)	La inicialización del procesador ingresó en un estado no recuperable
No recuperable	CPU Machine Chk: Processor sensor, transition to non-recoverable was asserted (Revisión de máquina de CPU: sensor de procesador, se confirmó la transición a un estado no recuperable)	La revisión de máquina del procesador ingresó en un estado no recuperable
Crítico	Memory Spared: Memory sensor, redundancy lost (<DIMM Location>) was asserted (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	Memory Mirrored: Memory sensor, redundancy lost (<DIMM Location>) was asserted (Memoria reflejada: Sensor de memoria, se confirmó la pérdida de redundancia (<Ubicación del módulo DIMM>))	La memoria reflejada ya no es redundante
Crítico	Memory RAID: Memory sensor, redundancy lost (<DIMM Location>) was asserted (RAID de memoria: sensor de memoria, se confirmó la pérdida de redundancia (<ubicación del DIMM>))	La memoria de RAID ya no es redundante
Advertencia	Memory Added: Memory sensor, presence (<DIMM Location>) was deasserted (Se agregó memoria: sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>))	Se retiró el módulo de memoria agregado
Advertencia	Memory Removed: Memory sensor, presence (<DIMM Location>) was deasserted (Se quitó la memoria: sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>))	Se retiró el módulo de memoria
Crítico	Memory Cfg Err: Memory sensor, configuration error (<DIMM Location>) was asserted (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	Mem Redun Gain: Memory sensor, redundancy degraded (<DIMM Location>) was asserted (Ganancia de redundancia de memoria: Sensor de memoria, se confirmó la redundancia degradada (<Ubicación del módulo DIMM>))	La redundancia de la memoria se ha degradado pero no se ha perdido

Crítico	PCIE Fatal Err: Critical Event sensor, bus fatal error was asserted (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	Chipset Err: Critical Event sensor, PCI PERR was asserted (Error de chipset: sensor de sucesos críticos, se confirmó un PERR de PCI)	Se detectó un error de chip
Advertencia	Mem ECC Warning: Memory sensor, transition to non-critical from OK (<DIMM Location>) was asserted (Advertencia de memoria ECC: sensor de memoria, se confirmó la transición de buen estado a estado no crítico (<ubicación del DIMM>))	Los errores corregibles ECC han aumentado por encima de la frecuencia normal
Crítico	Mem ECC Warning: Memory sensor, transition to critical from less severe (<DIMM Location>) was asserted (Advertencia de memoria ECC: sensor de memoria, se confirmó la transición de un estado crítico a uno menos grave (<ubicación del DIMM>))	Los errores ECC corregibles han alcanzado una frecuencia crítica
Crítico	POST Err: POST sensor, No memory installed (Error de la POST: sensor de la POST, no hay memoria instalada)	No se detectó memoria en la placa
Crítico	POST Err: POST sensor, Memory configuration error (Error de la POST: sensor de la POST, error de configuración de memoria)	Se ha detectado la memoria, pero no se puede configurar
Crítico	POST Err: POST sensor, Unusable memory error (Error de la POST: sensor de la POST, error de memoria inutilizable)	Se ha configurado la memoria, pero no se puede utilizar
Crítico	POST Err: POST sensor, Shadow BIOS failed (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	POST Err: POST sensor, CMOS failed (Error de la POST: sensor de la POST, falló el CMOS)	Error de CMOS
Crítico	POST Err: POST sensor, DMA controller failed (Error de la POST: sensor de la POST, falló el controlador de DMA)	Error del controlador de DMA
Crítico	POST Err: POST sensor, Interrupt controller failed (Error de la POST: sensor de la POST, falló el controlador de interrupción)	Error del controlador de interrupción
Crítico	POST Err: POST sensor, Timer refresh failed (Error de la POST: sensor de la POST, falló la actualización del temporizador)	Error de actualización del temporizador
Crítico	POST Err: POST sensor, Programmable interval timer error (Error de la POST: sensor de la POST, error de temporizador de intervalos programable)	Error del temporizador de intervalos programable
Crítico	POST Err: POST sensor, Parity error (Error de la POST: sensor de la POST, error de paridad)	Error de paridad
Crítico	POST Err: POST sensor, SIO failed (Error de la POST: sensor de la POST, falló el SIO)	Error de SIO
Crítico	POST Err: POST sensor, Keyboard controller failed (Error de la POST: sensor de la POST, falló el controlador de teclado)	Keyboard controller failure
Crítico	POST Err: POST sensor, System management interrupt initialization failed (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	POST Err: POST sensor, BIOS shutdown test failed (Error de la POST: sensor de la POST, falló la prueba de apagado del BIOS)	Error de la prueba de apagado del BIOS
Crítico	POST Err: POST sensor, BIOS POST memory test failed (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	POST Err: POST sensor, Dell remote access controller configuration failed (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	POST Err: POST sensor, CPU configuration failed (Error de la POST: sensor de la POST, falló la configuración de la CPU)	Error de configuración de la CPU
Crítico	POST Err: POST sensor, Incorrect memory configuration (Error de la POST: sensor de la POST, configuración incorrecta de la memoria)	Configuración incorrecta de la memoria
Crítico	POST Err: POST sensor, POST failure (Error de la POST: sensor de la POST, falló la POST)	Error general tras el vídeo
Crítico	Hdwar version err: Version Change sensor, hardware incompatibility was asserted (Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware)	Se detectó hardware incompatible
Crítico	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware) was asserted (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	Hdwar version err: Version Change sensor, hardware incompatibility (BMC firmware and CPU mismatch) was asserted (Error de versión del hardware: sensor de cambios de versión, se confirmó la incompatibilidad del hardware (incorrespondencia entre la CPU y el firmware del BMC))	La CPU y el firmware no son compatibles
Crítico	Mem Overtemp: Memory sensor, correctable ECC <DIMM Location> was asserted (Sobrecalentamiento de memoria: sensor de memoria, se confirmó un ECC corregible <ubicación del DIMM>)	Sobrecalentamiento del módulo de memoria

Crítico	Mem Fatal SB CRC: Memory sensor, uncorrectable ECC was asserted (CRC fatal de SB de memoria: sensor de memoria, se confirmó un ECC incorregible)	Falló la memoria de puente Sur
Crítico	Mem Fatal NB CRC: Memory sensor, uncorrectable ECC was asserted (CRC fatal de NB de memoria: sensor de memoria, se confirmó un ECC incorregible)	Falló la memoria de puente Norte
Crítico	WatchDog Timer: Watchdog sensor, reboot was asserted (Temporizador de vigilancia: sensor de vigilancia, se confirmó el reinicio)	El temporizador de vigilancia hizo que el sistema se reiniciara
Crítico	WatchDog Timer: Watchdog sensor, timer expired was asserted (Temporizador de vigilancia: sensor de vigilancia, se confirmó la expiración del temporizador)	El temporizador de vigilancia expiró pero no se realizó ninguna acción
Advertencia	Link Tuning: Version Change sensor, successful software or F/W change was deasserted (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	Link Tuning: Version Change sensor, successful hardware change <device slot number> was deasserted (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	LinkT/FlexAddr: Link Tuning sensor, failed to program virtual MAC address (Bus # Device # Function #) was asserted (FlexAddr/Link: sensor de ajuste de vínculo, se confirmó el error de programación de la dirección MAC virtual (n.° de bus, n.° de dispositivo, n.° de función))	No se pudo programar la dirección flexible para este dispositivo
Crítico	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz <location>) was asserted (LinkT/FlexAddr: sensor de ajuste de vínculo, se confirmó el error de la ROM de opción para apoyar el ajuste de vínculo o la dirección flexible (tarjeta intermediaria <ubicación>))	La ROM de opción no admite la dirección flexible ni el ajuste de vinculación
Crítico	LinkT/FlexAddr: Link Tuning sensor, failed to get link tuning or flex address data from BMC/iDRAC6 was asserted (LinkT/FlexAddr: sensor de ajuste de vínculo, se confirmó un error para obtener datos de ajuste de vínculo o de FlexAddress del BMC/iDRAC6)	No se pudo obtener información de ajuste de vinculación ni FlexAddress del BMC/iDRAC6
Crítico	LinkT/FlexAddr: Link Tuning sensor, device option ROM failed to support link tuning or flex address (Mezz XX) was asserted (FlexAddr/Link: sensor de ajuste de vínculo, se confirmó el error de la ROM de opción para apoyar el ajuste de vínculo o FlexAddress (tarjeta intermediaria XX))	Este evento se genera cuando la opción ROM del dispositivo PCI para una NIC no es compatible con la función de ajuste de vínculo o FlexAddress
Crítico	LinkT/FlexAddr: Link Tuning sensor, failed to program the virtual MAC address (<location>) was asserted (FlexAddr/Link: sensor de ajuste de vínculo, se confirmó un error en la programación de la dirección MAC virtual (<ubicación>))	Este evento se genera cuando el BIOS no puede programar la dirección MAC virtual en un dispositivo NIC específico
Crítico	I/O Fatal Err: Fatal IO Group sensor, fatal IO error (<location>) (Error fatal E/S: sensor de grupo ES fatal, error ES fatal (<ubicación>))	Este evento se genera en relación con un IERR de CPU e indica qué dispositivo causó el IERR de CPU
Advertencia	PCIE NonFatal Er: Non Fatal I/O Group sensor, PCIe error (<location>) (Error no fatal PCIE: sensor de grupo E/S no fatal, error PCIe (<ubicación>))	Este evento se genera en relación con un IERR de CPU

Visualización del registrodel iDRAC6

El **Registro del iDRAC6** es un registro permanente que se conserva en el firmware de iDRAC6. El registro contiene una lista de las acciones de usuario (como inicio y cierre de sesión y cambios de las políticas de seguridad) y de las alertas generadas por el iDRAC6. Cuando el registro se llena, las anotaciones más antiguas se sobrescriben.

El **Registro de sucesos del sistema** (SEL) contiene anotaciones de sucesos que ocurren en el servidor administrado y el **Registro del iDRAC** contiene anotaciones de sucesos que ocurren en el iDRAC6.

Para acceder al **registro del iDRAC**, realice los pasos siguientes:

- Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC** y después haga clic en **Registro del iDRAC**.

El **Registro del iDRAC** proporciona la información que aparece en la tabla 17-9.

Tabla 17-9. Información del registro del iDRAC6

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, 19 de dic. 16:55:47). El iDRAC6 obtiene la hora del reloj del servidor administrado. Cuando el iDRAC6 se inicie y no pueda comunicarse con el servidor administrado, la hora aparecerá como la cadena de Inicio del sistema.
Origen	La interfaz que ocasionó el suceso.
Descripción	Una breve descripción del suceso y el nombre de usuario que inició sesión en el iDRAC6.

Uso de los botones del registro del iDRAC6

La pantalla **Registro del iDRAC** tiene los siguientes botones (consulte la tabla 17-10).

Tabla 17-10. Botones del registro del iDRAC6

Botón	Acción
Imprimir	Imprime la pantalla **Registro del iDRAC**.
Borrar registro	Borra las anotaciones del **Registro del iDRAC**. **NOTA:** El botón **Borrar registro** sólo aparecerá si usted tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **Registro del iDRAC** en un directorio de su elección. **NOTA:** Si al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización acumulada de seguridad para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en **support.microsoft.com**.
Actualizar	Vuelve a cargar la pantalla **Registro del iDRAC**.

Cómo ver la información del sistema

La pantalla **Resumen del sistema** muestra la información sobre los siguientes componentes del sistema:

- Gabinete del sistema principal
- Integrated Dell Remote Access Controller

Para acceder a la información del sistema, haga clic en **Sistema**→ **Propiedades**.

Gabinete del sistema principal

La tabla 17-11 y la tabla 17-12 describen las propiedades del chasis de sistema principal.

Tabla 17-11. Campos de la información del sistema

Campo	Descripción
Descripción	Proporciona una descripción del sistema.
Versión del BIOS	Muestra la versión del BIOS del sistema.
Etiqueta de servicio	Muestra el número de la etiqueta de servicio del sistema.
Nombre de host	Proporciona el nombre del sistema host.
Nombre del sistema operativo	Muestra el sistema operativo que se ejecuta en el sistema.

Tabla 17-12. Campos de recuperación automática

Campo	Descripción
Acción de recuperación	Cuando se detecta un *bloqueo de sistema*, el iDRAC6 se puede configurar para que ejecute una de las acciones siguientes: **Sin acción**, **Restablecimiento forzado**, **Apagar** o **Ciclo de encendido**.
Cuenta regresiva inicial	El número de segundos después que se detecta un *bloqueo de sistema* al término de los cuales el iDRAC6 ejecutará una acción de recuperación.
Cuenta regresiva actual	El valor actual, en segundos, del temporizador de cuenta regresiva.

Integrated Dell Remote Access Controller

La tabla 17-13 describe las propiedades del iDRAC6.

Tabla 17-13. Campos informativos del iDRAC6

Campo	Descripción
Fecha/Hora	Proporciona la fecha y hora actuales en el iDRAC6 en el formato de hora media de Greenwich.
Versión del firmware	Enumera la versión del firmware del iDRAC6.

Firmware actualizado	Enumera la fecha en la que el firmware se ha actualizado por última vez. La fecha se muestra en formato UTC, por ejemplo: Jue, 8 de mayo de 2007, 22:18:21 UTC.
Dirección IP	La dirección de 32 bits que identifica la interfaz de red. El valor se muestra en formato de *números separados con puntos*, por ejemplo, 143.166.154.127.
predeterminada	La dirección IP de la puerta de enlace que actúa como vínculo a otras redes. Este valor está en formato de *números separados con puntos*, por ejemplo, 143.166.150.5.
Máscara de subred	La máscara de subred identifica las partes de la dirección IP que forman el prefijo extendido de red y el número de host. El valor se muestra en formato de *números separados con puntos*, por ejemplo, 255.255.0.0.
MAC Address	La dirección de Control de acceso a medios (MAC) que identifica de manera exclusiva a cada NIC en una red, por ejemplo: 00-00-0c-ac-08. Ésta es una identificación asignada por Dell y no se puede modificar.
DHCP activado	**Activado** indica que el protocolo de configuración dinámica de host (DHCP) está activado. **Desactivado** indica que DHCP *no* está activado.

Identificación del servidor administrado en el chasis

El chasis PowerEdge M1000e alberga hasta dieciséis servidores. Para localizar a un servidor específico en el chasis, puede usar la interfaz web del iDRAC6 para activar un parpadeo del LED del servidor en color azul. Cuando active el LED, puede especificar el número de segundos que desea que el LED parpadee para asegurarse que podrá localizar el chasis mientras el LED aún esté parpadeando. Si introduce **0**, el LED parpadeará hasta que usted lo desactive.

Para identificar el servidor:

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Solución de problemas**.
2. En la pantalla **Identificar**, seleccione **Identificar servidor**.
3. En el campo **Tiempo de espera para identificar el servidor**, introduzca el número de segundos que desea que el LED parpadee. Introduzca **0** si desea que el LED siga parpadeando hasta que usted lo desactive.
4. Haga clic en **Aplicar.**

El LED del servidor parpadeará en color azul durante el número de segundos que usted haya especificado.

Si introduce **0** para dejar el LED parpadeando, siga estos pasos para desactivarlo:

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC**→ **Solución de problemas**.
2. En la pantalla **Identificar**, deseleccione **Identificar servidor**.
3. Haga clic en **Aplicar.**

Uso de la consola de diagnósticos

El iDRAC6 proporciona un conjunto estándar de herramientas de diagnóstico de red (consulte la tabla 17-14) que son similares a las herramientas que se incluyen con los sistemas con Microsoft® Windows® o Linux. Por medio de la interfaz web de iDRAC6, se puede acceder a las herramientas de depuración de red.

Para tener acceso a la pantalla **Consola de diagnósticos**, realice los pasos a continuación:

1. Haga clic en **Sistema**→ **iDRAC**→ **Solución de problemas**.
2. Haga clic en la ficha **Diagnósticos**.

La tabla 17-14 describe los comandos que se pueden introducir en la pantalla **Consola de diagnósticos**. Introduzca un comando y haga clic en **Enviar**. Los resultados de depuración aparecerán en la pantalla **Consola de diagnósticos**.

Haga clic en el botón **Borrar** para borrar los resultados generados por el comando anterior.

Para actualizar la pantalla **Consola de diagnósticos**, haga clic en **Actualizar**.

Tabla 17-14. Comandos de diagnóstico

Comando	Descripción
arp	Muestra el contenido de la tabla del Protocolo para resolución de direcciones (ARP). Las anotaciones del ARP no se pueden agregar ni eliminar.
ifconfig	Muestra el contenido de la tabla de interfaz de red.
netstat	Imprime el contenido de la tabla de enrutamiento.
ping *<dirección IP>*	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se debe escribir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de

	control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de enrutamiento actual.
gettracelog	Muestra el registro de rastreo de iDRAC6. Consulte "gettracelog" para obtener más información.

Administración de alimentación en un sistema remoto

El iDRAC6 permite realizar de manera remota varias acciones de administración de alimentación en el servidor administrado. Use la pantalla **Administración de la alimentación** para realizar un apagado ordenado por medio del sistema operativo al reiniciar, encender y apagar el sistema.

NOTA: Debe tener permiso para **Ejecutar comandos de acción de servidor** para realizar acciones de administración de alimentación. Consulte "Cómo agregar y configurar usuarios de iDRAC6" para obtener ayuda con la configuración de permisos de usuario.

1. Haga clic en **Sistema** y después haga clic en la ficha **Administración de la alimentación**.
2. Seleccione una **Acción de control de alimentación**, por ejemplo, **Restablecer el sistema (reinicio mediante sistema operativo)**. La tabla 17-15 contiene información sobre las acciones de control de alimentación.
3. Haga clic en **Aplicar** para realizar la acción seleccionada.
4. Para continuar, haga clic en el botón correspondiente. Vea la tabla 17-15.

Tabla 17-15. Acciones de control de alimentación

Encender el sistema	Enciende la alimentación del sistema (equivalente a oprimir el botón de encendido cuando el sistema está apagado).
Apagar el sistema	Apaga la alimentación del sistema (equivalente a oprimir el botón de encendido cuando el sistema encendido).
NMI (Interrupción no enmascarable)	Envía una interrupción de alto nivel al sistema operativo, lo cual hace que el sistema detenga la operación para permitir actividades fundamentales de diagnóstico o solución de problemas.
Apagado ordenado	Intenta cerrar de manera estructurada el sistema operativo y luego apaga el sistema. Requiere un sistema operativo con ACPI (Interfaz de energía y configuración avanzada), lo cual permite que el sistema dirija la administración de la alimentación. **NOTA:** Puede que no sea posible realizar un apagado ordenado del sistema operativo del servidor cuando el software del servidor deja de responder o si no inició sesión como administrador en la consola local de Windows. En estos casos, deberá especificar la ejecución de un reinicio forzado en lugar de un apagado ordenado de Windows. Además, según la versión del sistema operativo Windows, puede existir una política configurada respecto del proceso de apagado que modifique el apagado cuando éste se inicie a partir del iDRAC6. Consulte la documentación de Microsoft que se refiere a la política del equipo local "Apagado: Permitir que el sistema se apague sin tener que iniciar sesión".
Restablecer el sistema (reinicio mediante sistema operativo)	Reinicia el sistema sin apagarlo (reinicio mediante sistema operativo).
Realizar ciclo de encendido del sistema	Apaga el sistema y después lo reinicia (reinicio mediante suministro de energía).

Tabla 17-16. Botones de administración de alimentación

Botón	**Acción**
Imprimir	Imprime los valores de la **Administración de la alimentación** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **Administración de la alimentación**.
Aplicar	Guarda cualquier configuración nueva que asigne mientras esté en la pantalla Administración de la alimentación.

Solución de problemas y preguntas frecuentes

La tabla 17-17 contiene la preguntas frecuentes sobre problemas de solución de problemas.

Tabla 17-17. Preguntas frecuentes/solución de problemas

Pregunta	**Respuesta**
El indicador LED del servidor parpadea en color ámbar.	Revise el registro de sucesos del sistema en busca de mensajes y después bórrelo para detener el parpadeo del indicador LED. En la interfaz web del iDRAC6: • Consulte "Consulta del registro de sucesos del sistema (SEL)". En SM-CLP: • Consulte "Administración del registro de sucesos del sistema".

	En la utilidad de configuración del iDRAC6: • Consulte "Menú del registro de sucesos del sistema". O bien:
Hay un LED que parpadea de color azul en el servidor.	Un usuario ha activado la identificación de localizador del servidor. Ésta es una señal para ayudar a identificar el servidor en el chasis. Consulte "Identificación del servidor administrado en el chasis" para obtener información sobre esta función.
¿Cómo puedo encontrar la dirección IP del iDRAC6?	En la interfaz web del CMC: 1. Haga clic en **Chasis**→ **Servidores** y después haga clic en la ficha **Configuración**. 2. Haga clic en **Instalar**. 3. Lea la dirección IP del servidor en la tabla que aparece. En el iKVM: • Reinicie al servidor e introduzca la utilidad de configuración del iDRAC6 presionando <Ctrl><E>. O bien: • Espere a que la dirección IP aparezca durante la POST del BIOS. O bien: • Seleccione la consola "Dell CMC" consola en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *Guía del usuario del firmware del CMC* para una lista completa de los subcomandos RACADM del CMC. También puede usar el comando local **getsysinfo** de RACADM para ver la dirección IP del iDRAC6.
	Por ejemplo: $ racadm getniccfg -m server-1 DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1 En RACADM local: 1. Introduzca el comando siguiente en una petición de comandos: racadm getsysinfo En la pantalla LCD: 1. En el menú principal, marque **Servidor** y presione el botón de verificación. 2. Seleccione el servidor cuya dirección IP busca y presione el botón de verificación.
¿Cómo puedo encontrar la dirección IP del CMC?	En la interfaz web del iDRAC6: • Haga clic en **Sistema**→ **Acceso remoto**→ **CMC**. La dirección IP del CMC se muestra en la pantalla **Resumen**. O bien: • Seleccione la consola "Dell CMC" consola en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *Guía del usuario del firmware del CMC* para una lista completa de los subcomandos RACADM del CMC. $ racadm getniccfg -m chassis NIC Enabled = 1 DHCP Enabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Current Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate
La conexión de red del iDRAC6 no funciona.	• Asegúrese de que el cable de la LAN esté conectado con el CMC. • Asegúrese de que la LAN del iDRAC6 esté activada.
Inserté el servidor en el chasis y presioné el botón de encendido, pero no pasó nada.	• El iDRAC6 requiere alrededor de 30 segundos para inicializarse antes de que el servidor se pueda encender. Espere durante 30 segundos y luego presione el botón de encendido otra vez. • Revise el presupuesto de alimentación del CMC. Es posible que el presupuesto de alimentación del chasis se haya excedido.
Olvidé el nombre del usuario administrativo del iDRAC6 y la contraseña.	Deberá restaurar los valores predeterminados del iDRAC6. 1. Reinicie el servidor y presione <Ctrl><E> cuando se le solicite para ingresar en la utilidad de

	configuración del iDRAC6. 2. En el menú **Utilidad de configuración**, marque **Restablecer los valores predeterminados** y presione <Entrar>. Para obtener más información, consulte "Restablecer valores predeterminados".
¿Cómo puedo cambiar el nombre de la ranura de mi servidor?	1. Inicie sesión en la interfaz web del CMC. 2. Abra el árbol **Chasis** y haga clic en **Servidores**. 3. Haga clic en la ficha **Configuración**. 4. Introduzca el nuevo nombre para la ranura en la fila del servidor. 5. Haga clic en **Aplicar**.
Cuando se inicie una sesión de redirección de consola en la interfaz web del iDRAC6, aparecerá una ventana emergente de seguridad de ActiveX.	Es posible que el iDRAC6 no sea un sitio de confianza en el explorador de cliente. Para evitar que la ventana emergente de seguridad aparezca cada vez que usted comience una sesión de redirección de consola, agregue el iDRAC6 a la lista de sitios de confianza: 1. Haga clic en **Herramientas**→ **Opciones de Internet...**→ **Seguridad**→ **Sitios de confianza**. 2. Haga clic en **Sitios** e introduzca la dirección IP o el nombre DNS del iDRAC6. 3. Haga clic en **Add** (Agregar).
Cuando inicio una sesión de redirección de consola, la pantalla del visor está en blanco.	Si usted tiene privilegio de **Medios virtuales**, pero no privilegio de **Redirección de consola**, podrá iniciar el visor para que pueda acceder a la función de medios virtuales, pero la consola del servidor administrado no aparecerá.
El iDRAC6 no se inicia.	Retire el servidor e insértelo nuevamente. Revise la interfaz web del CMC para ver si el iDRAC6 aparece como componente que se puede actualizar. Si lo hace, siga las instrucciones de la sección "Actualización del firmware del iDRAC6 por medio del CMC". Si esto no corrige el problema, póngase en contacto con el personal de asistencia técnica.
Cuando trato de iniciar el servidor administrado, el indicador de alimentación es de color verde, pero no hay POST ni vídeo.	Esto puede pasar si se presenta cualquiera de las condiciones siguientes: - La memoria no está instalada o no se puede acceder a ella. - La CPU no está instalada o no se puede tener acceso a ella. - La tarjeta de vídeo está ausente o no está conectada correctamente. Asimismo, busque mensajes de error en el registro del iDRAC6 desde la interfaz web del iDRAC6 o en la pantalla LCD.

Regresar a la página de contenido

Regresar a la página de contenido

Glosario

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

Active Directory

Active Directory es un sistema centralizado y estandarizado que automatiza la administración de red de los datos de usuario, la seguridad y los recursos distribuidos y hace posible las operaciones con otros directorios. Active Directory está diseñado específicamente para los entornos de red distribuidos.

AGP

Siglas de accelerated graphics port (puerto de gráficos acelerados), que es una especificación de bus que permite que las tarjetas de gráficos accedan más rápido a la memoria del sistema principal.

ARP

Siglas de Address Resolution Protocol (protocolo para resolución de direcciones), que es un método para encontrar la dirección Ethernet de un host a partir de su dirección de Internet.

ASCII

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

BIOS

Siglas de basic input/output system (sistema básico de entradas y salidas), que es la parte del software de sistema que proporciona la interfaz al nivel más bajo a los dispositivos periféricos y que controla la primera fase del proceso de inicio del sistema, incluyendo la instalación del sistema operativo en la memoria.

bus

Conjunto de conductores que conectan las distintas unidades funcionales en un equipo. Los buses reciben su nombre en función del tipo de datos que llevan, por ejemplo, bus de datos, bus de direcciones o bus de PCI.

CA

Una autoridad de certificados es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis fiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de CA se incluyen Thawte y VeriSign. Después de recibir la solicitud CSR, la autoridad de certificados (CA) revisa y verifica la información que contiene. Si el candidato cumple los estándares de seguridad de la autoridad de certificados, ésta emite un certificado al candidato que lo identifica de forma exclusiva para transacciones a través de redes y en Internet.

captura SNMP

Notificación (suceso) generada por el iDRAC6 o el CMC que contiene información sobre los cambios de estado en el sistema administrado o sobre problemas potenciales de hardware.

CD

Siglas de compact disc (disco compacto).

CHAP

Siglas de Challenge-Handshake Authentication Protocol (Protocolo de autenticación de establecimiento de conexión por desafío), un esquema de autenticación utilizado por los servidores PPP para validar la identidad del iniciador de la conexión.

CIM

Sigla de Common Information Model (Modelo de información común), que es un protocolo diseñado para la administración de sistemas en una red.

CLI

Siglas de command-line interface (interfaz de línea de comandos).

CLP

Siglas de command-line protocol (protocolo de línea de comandos).

CMC

Siglas de "Enclosure Management Controller" (Controlador de administración de gabinete) que es la interfaz de controlador entre el iDRAC6 y el CMC del sistema administrado.

CSR

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

DDNS

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

DHCP

Siglas de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host), que es un protocolo que proporciona los medios para distribuir direcciones IP de manera dinámica a los equipos en una red de área local.

Dirección MAC

Abreviatura para dirección "media access control" (control de acceso a medios), que es una dirección única incorporada en los componentes físicos de una NIC.

disco RAM

Programa residente en la memoria que emula una unidad de disco duro. El iDRAC6 mantiene un disco RAM en su memoria.

DLL

Siglas de Dynamic Link Library (Biblioteca de enlaces dinámicos) que es una biblioteca de pequeños programas a los que un programa más grande que se ejecuta en el sistema puede llamar cuando sea necesario. El programa pequeño que permite al programa más grande comunicarse con un dispositivo específico, como una impresora o un escáner, a menudo se empaqueta como un programa (o archivo) DLL.

DMTF

Siglas de Distributed Management Task Force (Equipo de trabajo de administración distribuida).

DNS

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

DSU

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

esquema ampliado

Solución que se usa con Active Directory para determinar el acceso de los usuarios al iDRAC6; usa objetos de Active Directory definidos por Dell.

esquema estándar

Solución que se usa con Active Directory para determinar el acceso de los usuarios al iDRAC6; utiliza únicamente objetos de grupo de Active Directory.

estación de administración

La estación de administración es un sistema que accede de forma remota al iDRAC6.

FQDN

Siglas de Fully Qualified Domain Names (nombres de dominio completos). Microsoft® Active Directory® sólo admite nombres de dominio completos de 64 bytes o menos.

FSMO

Flexible Single Master Operation (Operación maestra única y flexible). Es la manera en la que Microsoft garantiza la atomicidad de la operación de ampliación.

GMT

Abreviatura de Greenwich Mean Time (hora media de Greenwich), que es la hora estándar común a todos los lugares en el mundo. La GMT refleja nominalmente la hora solar media sobre el meridiano principal (longitud 0) que atraviesa el observatorio de Greenwich en las afueras de Londres, Reino Unido.

GPIO

Abreviatura de general purpose input/output (entrada/salida de propósito general).

GRUB

Abreviatura de GRand Unified Bootloader, un cargador nuevo de Linux de uso común.

GUI

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

hardware log

Registra los sucesos generados por el iDRAC6 y el CMC.

iAMT

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

ICMB

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

ICMP

Siglas de Internet control message protocol (protocolo de mensajes de control de Internet).

ID

Abreviatura para identificación, usada comúnmente al referirse a la identificación de un usuario (Id. del usuario) o identificación de un objeto (Id. del objeto).

iDRAC6

Siglas de Dell Remote Access Controller 6 Enterprise.

iDRAC6

Siglas de Integrated Dell Remote Access Controller 6, el sistema de supervisión y control integrado en el chip de los servidores Dell 10G PowerEdge.

IP

Abreviatura de Internet Protocol (protocolo de Internet), que es un nivel de red de TCP/IP. El IP proporciona enrutamiento, fragmentación y reensamblaje de paquetes.

IPMB

Siglas de intelligent platform management bus (bus de administración de plataforma inteligente), que es un bus que se utiliza en la tecnología de administración de sistemas.

IPMI

Abreviatura de Intelligent Platform Management Interface (interfaz de administración de plataformas inteligentes), que es una parte de la tecnología de administración de sistemas.

Kbps

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

LAN

Abreviatura de local area network (red de área local).

LDAP

Abreviatura de protocolo ligero de acceso a directorios.

LED

Abreviatura de diodo emisor de luz.

LOM

Abreviatura de local area network on motherboard (red de área local integrada a la placa base).

MAC

Siglas de media access control (control de acceso a medios), que es un subnivel de red entre un nodo de red y el nivel físico de la red.

MAP

Siglas de Manageability Access Point (Punto de acceso de administrabilidad).

Mbps

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

MIB

Abreviatura de management information base (base de información de administración).

MII

Siglas de Media Independent Interface (Interfaz independiente de medios).

NAS

Abreviatura de network attached storage (almacenamiento conectado a red).

NIC

Siglas de network interface card (tarjeta de interfaz de red). Una placa adaptadora de circuitos instalada en un equipo para brindar una conexión física con la red.

OID

Abreviatura de Object Identifiers (identificadores de objeto).

OSCAR

Siglas de "On Screen Configuration and Reporting" (Configuración e informes en pantalla). OSCAR es el menú que Avocent iKVM muestra cuando usted presiona <Impr Pant>. Permite seleccionar la consola del CMC o la consola del iDRAC6 para un servidor instalado en el CMC.

PCI

Abreviatura de Peripheral Component Interconnect (interconexión de componentes periféricos), que es una interfaz y tecnología de bus estándar para la conexión de periféricos a un sistema y para la comunicación con esos periféricos.

POST

Siglas de power-on self-test (autoprueba de encendido), que es una secuencia de pruebas de diagnóstico que un sistema ejecuta automáticamente cuando se enciende.

PPP

Abreviatura de "Point-to-Point Protocol" (protocolo punto a punto), que es el protocolo estándar de Internet para transmitir datagramas de la capa de red (como paquetes IP) sobre vínculos punto a punto en serie.

RAC

Abreviatura de remote access controller (controlador de acceso remoto).

RAM

Siglas de memoria de acceso aleatorio. La RAM es una memoria de propósito general que se puede leer y escribir en los sistemas y en el iDRAC6.

redirección de consola

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

ROM

Siglas de read-only memory (memoria de sólo lectura), que es la memoria desde la cual es posible leer los datos, pero no se pueden escribir en ella.

RPM

Abreviatura de Red Hat® Package Manager (administrador de paquetes Red Hat), que es un sistema de administración de paquetes para el sistema operativo Red Hat Enterprise Linux® que ayuda con la instalación de paquetes de software. Es similar a un programa de instalación.

SAC

Siglas de Special Administration Console (consola de administración especial) de Microsoft.

SAI

Abreviatura de sistema de energía ininterrumpida.

SAP

Siglas de Service Access Point (Punto de acceso de servicio).

SEL

Siglas de registro de sucesos del sistema.

servidor administrado

El servidor administrado es el sistema al que está incorporado el iDRAC6.

SMI

Abreviatura de systems management interrupt (interrupción de administración del sistema).

SMTP

Abreviatura de Simple Mail Transfer Protocol (Protocolo simple de transferencia de correo), un protocolo utilizado para transferir el correo electrónico entre sistemas, por lo general a través de Ethernet.

SMWG

Siglas de Systems Management Working Group (Grupo de trabajo de administración de sistemas).

SSH

Abreviatura para Secure SHell.

SSL

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

TAP

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

TCP/IP

Abreviatura de Transmission Control Protocol/Internet Protocol (protocolo de control de transmisiones/protocolo de Internet), que representa el conjunto de protocolos de Ethernet estándares que incluyen los protocolos del nivel de red y el nivel de transporte.

TFTP

Abreviatura de Trivial File Transfer Protocol (protocolo trivial de transferencia de archivos, que es un protocolo de transferencia simple usado para cargar código de inicio a los dispositivos o sistemas sin discos.

USB

Abreviatura de bus serial universal.

UTC

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

VLAN

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

VNC

Abreviatura de virtual network computing (cómputo de red virtual).

VT-100

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

WAN

Abreviatura de wide area network (red de área amplia).

Regresar a la página de contenido

Regresar a la página de contenido

Guía del usuario de Acceso remoto integrado Dell™ Controller 6 (iDRAC6) Enterprise para servidores del módulo de alta densidad versión 2.0

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

PRECAUCIÓN: Un mensaje de PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos si no se siguen las instrucciones.

Marzo 2009 Rev. A00

Regresar a la página de contenido