Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

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.

Diciembre de 2009

Regresar a la página de contenido

Generalidades de los subcomandos de RACADM

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

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

PRECAUCIÓN: El firmware más reciente del iDRAC6 admite únicamente la versión más reciente de RACADM. Es posible que encuentre errores si utiliza una versión anterior de RACADM para consultar el iDRAC6 que tiene el firmware más reciente. Instale la versión de RACADM que se incluye con el DVD Dell™ OpenManage™ 6.2.

---

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

Salida

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

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

config

La Tabla A-2 describe el subcomando **config**.

Tabla A-2. config/getconfig

Subcomando	Definición
config	Configura el iDRAC6.

Sinopsis

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

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

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.

NOTA: Consulte "Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6 Enterprise" para obtener información sobre el grupo y el objeto que se utilizarán con este comando.

Entrada

La Tabla A-3 describe las opciones del subcomando **config**.

Tabla A-3. Opciones y descripciones del subcomando config

Opción	Descripción
-f	La opción **-f** <*nombre_de_archivo*> 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.
-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 interfaz de línea de comandos 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

La Tabla A-4 describe 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 excepción para capturar el grupo **cfgIpmiPet** en el archivo. Además, en esta versión **cfgIpmiPet** y **cfgIpmiPef** se guardarán únicamente a través de RACADM Telnet/SSH y remoto y no mediante RACADM local.
-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 interfaz de línea de comandos de RACADM

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

NOTA: Consulte "Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6 Enterprise" para obtener información sobre el grupo y el objeto que se utilizarán con este comando.

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`

`racadm getconfig -g <nombre_de_grupo> -o <nombre_de_objeto>`

`[-i índice]`

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

getssninfo

La Tabla A-5 describe el subcomando **getssninfo**.

Tabla A-5. Subcomando getssninfo

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

Sinopsis

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

Descripción

El comando **getssninfo** muestra una lista de los usuarios que están conectados al 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)

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

Entrada

La Tabla A-6 describe las opciones del subcomando **getssninfo**.

Tabla A-6. Opciones del subcomando getssninfo

Opción	Descripción
-A	La opción **-A** elimina la impresión de los encabezados de los datos.
-u	La opción de nombre de usuario **-u** <*nombre_de_usuario*> limita la salida impresa a sólo registros detallados de la sesión para el nombre de usuario determinado. Si se proporciona un asterisco (*) como nombre de usuario, aparecerá una lista de todos los usuarios. La información de resumen no se imprime cuando se especifique esta opción.

Ejemplos

- `racadm getssninfo`

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

```
C:\>racadm -r 10.35.155.185 -u root -p calvin getssninfo

Security Alert: Certificate is invalid - Certificate is not signed by Trusted Third Party

Continuing execution. Use -S option for racadm to stop execution on certificate-related errors.

(Alerta de seguridad: Certificado no válido. El certificado no está firmado por un tercero de confianza

Ejecución continua. Utilice la opción -S para que racadm detenga la ejecución al producirse errores relacionados con certificados.)
```

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

Usuario	Dirección IP	Tipo
root	192.168.1.1	RACADM

---

getsysinfo

La Tabla A-8 describe el subcomando **racadm getsysinfo**.

Tabla A-8. getsysinfo

Comando	Definición
getsysinfo	Muestra información relacionada con iDRAC6.

Sinopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-4] [-6]
```

Descripción

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

Entrada

La Tabla A-9 describe 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.
-4	Muestra información de IPv4 del iDRAC6.
-6	Muestra información de IPv6 del iDRAC6.

Salida

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

NOTA: El subcomando de racadm *getsysinfo* local en Linux muestra la *longitud del prefijo* para la Dirección 2 de IPv6 a la dirección 15 de IPv6 y la dirección local del vínculo en líneas separadas.

Ejemplo del mensaje de salida

RAC Information:

RAC Date/Time = Tue Apr 15 03:52:56 2036

Firmware Version = 02.20

Firmware Build = 25

Last Firmware Update = Mon Oct 26 18:01:39 2009

Hardware Version = 0.0

MAC Address = 00:21:9b:fe:6b:21

Common settings:

Register DNS RAC Name = 0

DNS RAC Name = iDRAC-tt

Current DNS Domain =

Domain Name from DHCP = 1

IPv4 settings:

Enabled = 1

Current IP Address = 192.168.1.166

Current IP Gateway = 0.0.0.0

Current IP Netmask = 255.255.255.0

DHCP Enabled = 1

Current DNS Server 1 = 0.0.0.0

Current DNS Server 2 = 0.0.0.0

DNS Servers from DHCP = 1

IPv6 settings:

Enabled = 0

Current IP Address 1 = ::

Current IP Gateway = ::

Prefix Length = 64

Autoconfig = 0

Link Local IP Address = ::

Current IP Address 2 = ::

Current IP Address 3 = ::

Current IP Address 4 = ::

Current IP Address 5 = ::

Current IP Address 6 = ::

Current IP Address 7 = ::

Current IP Address 8 = ::

Current IP Address 9 = ::

Current IP Address 10 = ::

Current IP Address 11 = ::

Current IP Address 12 = ::

Current IP Address 13 = ::

Current IP Address 14 = ::

Current IP Address 15 = ::

DNS Servers from DHCPv6 = 0

Current DNS Server 1 = ::

Current DNS Server 2 = ::

System Information:

System Model = PowerEdge M710

System BIOS Version = 1.1.4

Service Tag = 2JWK22S

Host Name = WIN-IHF5D2BF5SN

OS Name = Microsoft Windows Server 2008 R2, Standard x64 Edition

Power Status = ON

Watchdog Information:

Recovery Action = None

Present countdown value = 0 seconds

Initial countdown value = 0 seconds

Embedded NIC MAC Addresses:

Ethernet NIC1 = 00:23:AE:EC:2E:38

iSCSI = 00:23:AE:EC:2E:39

Ethernet NIC2 = 00:23:AE:EC:2E:3A

iSCSI = 00:23:AE:EC:2E:3B

Ethernet NIC3 = 00:23:AE:EC:2E:3C

iSCSI = 00:23:AE:EC:2E:3D

Ethernet NIC4 = 00:23:AE:EC:2E:3E

iSCSI = 00:23:AE:EC:2E:3F

Ejemplos

```
racadm getsysinfo -A -s

"System Information:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON"

racadm getsysinfo -w -s
```

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

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

Restricciones

Los campos **Nombre del host** y **Nombre del sistema operativo** en el mensaje de **getsysinfo** muestran la información correcta sólo cuando Dell OpenManage Server Administrator está instalado en el servidor administrado. De lo contrario, es posible que estos campos aparezcan en blanco o muestren información incorrecta. Representan una excepción los nombres de sistemas operativos VMware®, que se muestran aun si Server Administrator no está instalado en el sistema administrado.

---

getractime

La Tabla A-10 describe el subcomando **getractime**.

Tabla A-10. getractime

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

Sinopsis

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

Descripción

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*, que es el mismo formato que genera el comando **date** de UNIX®.

Salida

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

Ejemplo del mensaje de salida

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20071208201542.000000
```

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

setniccfg

La Tabla A-11 describe el subcomando **setniccfg**.

Tabla A-11. setniccfg

Subcomando	Definición
setniccfg	Establece la configuración IP para el controlador.

Sinopsis

```
racadm setniccfg -d

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

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

Descripción

El subcomando **setniccfg** establece la dirección IP del 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 por completo. <*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
- RACADM remoto
- RACADM Telnet/SSH

---

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:

IPv4 settings:

```
NIC Enabled = 1

DHCP Enabled = 1

IP Address = 10.35.0.64

Subnet Mask = 255.255.255.0

Gateway = 10.35.0.1
```

IPv6 settings:

```
IPv6 Enabled = 0

DHCP6 Enabled = 0

IP Address 1 = ::

Prefix Length = 64

Gateway = ::

Link Local Address = ::

IP Address 2 = ::

IP Address 3 = ::

IP Address 4 = ::

IP Address 5 = ::

IP Address 6 = ::

IP Address 7 = ::

IP Address 8 = ::

IP Address 9 = ::

IP Address 10 = ::

IP Address 11 = ::

IP Address 12 = ::

IP Address 13 = ::

IP Address 14 = ::

IP Address 15 = ::
```

NOTA: La información IPv6 se muestra sólo si el iDRAC6 admite IPv6.

Interfaces admitidas

- RACADM local
- RACADM remoto

- RACADM Telnet/SSH

---

getsvctag

La Tabla A-13 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.

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

racreset

La Tabla A-14 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 dos minutos para volver a un estado utilizable.

Sinopsis

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

Descripción

El subcomando **racreset** restablece el iDRAC6. El suceso de restablecimiento se escribe en el registro del iDRAC6. El restablecimiento forzado realiza una operación de restablecimiento profunda en el iDRAC6. El restablecimiento forzado sólo debe utilizarse como último recurso para recuperar el iDRAC6. El restablecimiento ordenado realiza una operación de reinicio ordenado en iDRAC6.

Ejemplos

- `racadm racreset`

  Iniciar la secuencia de restablecimiento ordenado del iDRAC6.

- `racadm racreset hard`

  Iniciar la secuencia de restablecimiento forzado del iDRAC6.

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

racresetcfg

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

Tabla A-15. racresetcfg

Subcomando	Definición
racresetcfg	Restablece los valores predeterminados de fábrica de toda la configuración del iDRAC6. **NOTA:** El subcomando **racresetcfg** no restablece el objeto **cfgDNSRacName**.

Sinopsis

```
racadm racresetcfg
```

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

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, desactiva el DHCP 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

La Tabla A-16 describe el subcomando **serveraction**.

Tabla A-16. serveraction

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

Sinopsis

```
racadm serveraction <acción>
```

Descripción

El subcomando **serveraction** permite que los usuarios realicen operaciones de administración de la alimentación en el sistema host. La Tabla A-17 describe las

opciones de control de alimentación de **serveraction**.

Tabla A-17. Opciones del subcomando serveraction

Cadena	Definición
<*acción*>	Especifica la acción. Las opciones de la cadena <*acción*> son: • **powerdown**: Apaga el servidor administrado. • **powerup**: Enciende el servidor administrado. • **powercycle**: Realiza una operación de ciclo de encendido en el servidor administrado. Esta acción es similar a la acción de presionar el botón de encendido en el panel anterior del sistema para 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
- RACADM remoto
- RACADM Telnet/SSH

---

getraclog

La Tabla A-18 describe el comando **racadm getraclog**.

Tabla A-18. getraclog

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

Sinopsis

```
racadm getraclog -i

racadm getraclog [-A] [-o] [-c count] [-s start-record] [-m]
```

Descripción

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

-s	Especifica la anotación inicial a partir de la cual se muestra la información.

Salida

El mensaje de salida predeterminado muestra el número de entrada, 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 que el servidor administrado se inicia, la hora de sistema del mismo se usa para registrar la fecha y hora.

NOTA: Es probable que las anotaciones del Registro del RAC para *SystemBoot* que se muestran al usar el comando de racadm local, "racadm getraclog", no tengan el formato correcto. Por ejemplo, algunos caracteres adicionales podrían mostrarse en el campo "Descripción" o podría estar vacío el campo "Fuente".

Ejemplo del mensaje de salida

```
Entrada:          1
Fecha y hora:     8 dic 08:10:11
Origen:           inicio de sesión[433]
Descripción:      inicio de sesión de root proveniente de 192.168.1.1
```

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

clrraclog

Sinopsis

```
racadm clrraclog
```

Descripción

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

---

getsel

La Tabla A-20 describe el comando **getsel**.

Tabla A-20. getsel

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

Sinopsis

```
racadm getsel -i

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

Descripción

El comando **getsel -i** muestra el número de anotaciones en SEL.

Se utilizan las siguientes opciones de **getsel** (sin la opción **-i**) 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 la salida debe mostrarse sin encabezados ni etiquetas.
-c	Proporciona el recuento máximo de anotaciones a generar.
-o	Muestra la salida en una sola línea.
-s	Especifica el registro inicial que se utiliza para la muestra.
-E	Coloca los 16 bytes de SEL sin procesar al final de cada línea de salida como una secuencia de valores hexadecimales.
-R	Sólo imprime datos sin procesar.
-i	Muestra el número de anotaciones en SEL.
-m	Muestra una pantalla de información a la vez y pide al usuario que continúe (se parece al comando **more** de UNIX).

Salida

El mensaje de salida predeterminado muestra el número del registro, fecha y hora, gravedad y la descripción.

Por ejemplo:

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

clrsel

Sinopsis

```
racadm clrsel
```

Descripción

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

gettracelog

La Tabla A-22 describe el subcomando **gettracelog**.

Tabla A-22. gettracelog

Comando	Definición
gettracelog -i	Muestra la cantidad de entradas del **registro de rastreo del iDRAC6**.
gettracelog	Muestra el **registro de rastreo del iDRAC6**.

Sinopsis

```
racadm gettracelog -i

racadm gettracelog [-A] [-o] [-c count] [-s startrecord] [-m]
```

Descripción

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

Tabla A-23. Opciones del subcomando gettracelog

Opción	Descripción
-i	Muestra la cantidad de entradas del **registro de rastreo del iDRAC6**.
-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 entrada, 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 192.168.1.1: session timeout sid 0be0aef4
```

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

sslcsrgen

La Tabla A-24 describe el subcomando **sslcsrgen**.

Tabla A-24. sslcsrgen

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

Sinopsis

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

racadm sslcsrgen -s
```

Descripción

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

Opciones

La Tabla A-25 describe las opciones del subcomando **sslcsrgen**.

Tabla A-25. Opciones del subcomando sslcsrgen

Opción	Descripción
-g	Genera una nueva CSR.
-s	Muestra el estado del proceso de generación de la CSR (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
- RACADM remoto
- RACADM Telnet/SSH (sólo genera, no descarga. La opción **-f** no es aplicable)

---

sslcertupload

La Tabla A-26 describe el subcomando **sslcertupload**.

Tabla A-26. sslcertupload

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

Sinopsis

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

Opciones

La Tabla A-27 describe las opciones del subcomando **sslcertupload**.

Tabla A-27. Opciones del subcomando sslcertupload

Opción	Descripción
-t	Especifica el tipo de certificado que se va a cargar, ya sea el certificado de 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 es así.

Ejemplo

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

Interfaces admitidas

- RACADM local
- RACADM remoto

---

sslcertdownload

La Tabla A-28 describe el subcomando **sslcertdownload**.

Tabla A-28. sslcertdownload

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

Sinopsis

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

Opciones

La Tabla A-29 describe las opciones del subcomando **sslcertdownload**.

Tabla A-29. Opciones del subcomando sslcertdownload

Opción	Descripción
-t	Especifica el tipo de certificado que se va a descargar, sea 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
- RACADM remoto

---

sslcertview

La Tabla A-30 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

La Tabla A-31 describe las opciones del subcomando **sslcertview**.

Tabla A-31. Opciones del subcomando sslcertview

Opción	Descripción
-t	Especifica el tipo de certificado que se quiere ver, 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
- RACADM remoto
- RACADM Telnet/SSH

---

testemail

La Tabla A-32 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 <índice>
```

Descripción

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

Antes de ejecutar el comando `testemail`, asegúrese de que el servidor SMTP esté configurado y 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 *<índice>* donde *<índice>* es un número de 1 a 4

Opciones

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

Tabla A-34. Opción del subcomando testemail

Opción	Descripción
-i	Especifica el índice de la alerta por correo electrónico que se va a probar. El índice de **-i** puede ir del 1 al 4.

Salida

Éxito: Correo electrónico de prueba enviado exitosamente

Falla: No fue posible enviar el correo electrónico de prueba

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

testtrap

La Tabla A-35 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 para 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 los valores de captura de prueba	racadm getconfig -g cfgIpmiPet -i <índice> donde <*índice*> es un número de 1 a 4

Entrada

La Tabla A-37 describe las opciones del subcomando **testtrap**.

Tabla A-37. Opciones del subcomando testtrap

Opción	Descripción

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

vmdisconnect

Sinopsis

```
racadm vmdisconnect
```

Descripción

El subcomando **vmdisconnect** permite que el usuario desconecte la sesión de medios virtuales de otro usuario. Una vez desconectada, la interfaz web reflejará el estado de conexión correcto.

El subcomando **vmdisconnect** permite que un usuario del iDRAC6 desconecte todas las sesiones activas de medios virtuales. Las sesiones de medios virtuales activas pueden mostrarse en la interfaz web del iDRAC6 o mediante el subcomando **getsysinfo** de RACADM.

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

clearasrscreen

Sinopsis

```
racadm clearasrscreen
```

Descripción

Borra la pantalla de último bloqueo (ASR) Consulte "Configuración del servidor administrado para capturar la pantalla de último bloqueo" y "Desactivación de la opción de reinicio automático de Windows".

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

localconredirdisable

Sinopsis

```
racadm localconredirdisable <opción>
```

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

Descripción

Desactiva la redirección de consola a la estación de administración.

Valores legales

`0` = Activar

`1` = Desactivar

Interfaces admitidas

- RACADM local

---

fwupdate

NOTA: Para usar este comando, se debe tener permiso para **Configurar el iDRAC6**.

La Tabla A-38 describe el subcomando **fwupdate**.

Tabla A-38. fwupdate

Subcomando	Definición
fwupdate	Actualiza el firmware del iDRAC6

Sinopsis

```
racadm fwupdate -s

racadm fwupdate -g -u -a <dirección_IP_del_servidor_TFTP> [-d <ruta_de_acceso>]

racadm fwupdate -r
```

Descripción

El subcomando **fwupdate** permite que los usuarios actualicen el firmware del iDRAC6. El usuario puede:

- Revisar el estado del proceso de actualización del firmware
- Actualizar el firmware del iDRAC6 desde un servidor TFTP si se proporciona una dirección IP y una ruta de acceso opcional
- Reversión al firmware en espera

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

Entrada

La Tabla A-39 describe las opciones del subcomando **fwupdate**.

NOTA: La opción **-p** no se admite con la consola remota o Telnet/SSH. Además, la opción **-p** no se admite en los sistemas operativos Linux.

Tabla A-39. Opciones del subcomando fwupdate

Opción	Descripción
-u	La opción **actualizar** ejecuta una suma de comprobación del archivo de actualización del firmware y comienza el verdadero proceso de actualización. Esta opción se puede usar junto con las opciones **-g** o **-p**. Al final de la actualización, el iDRAC6 realiza un restablecimiento parcial.
-s	La opción **estado** muestra el estado actual del avance del proceso de actualización. Esta opción siempre se usa sin otras opciones.
-g	La opción **obtener** hace que el firmware obtenga el archivo de actualización del servidor TFTP. El usuario también debe especificar las opciones **-a** y **-d**. A falta de la opción **-a**, se leen los valores predeterminados de las propiedades que se encuentran en el grupo **cfgRemoteHosts** y se utilizan las propiedades **cfgRhostsFwUpdateIpAddr** y **cfgRhostsFwUpdatePath**.
-a	La opción **Dirección IP** especifica la dirección IP del servidor TFTP.
-d	La opción **-d**, u opción de **directorio**, especifica el directorio en el servidor TFTP o en el servidor del host del iDRAC6 donde reside el archivo de actualización del firmware.
-r	La opción **reversión** se usar para realizar una reversión hasta el firmware en espera.

Salida

Muestra un mensaje que indica qué operación se está ejecutando.

Ejemplos

- `racadm fwupdate -g -u -a 192.168.1.1 -d <ruta de acceso>`

  En este ejemplo, la opción **-g** hace que el firmware descargue el archivo de actualización de firmware de una ubicación (que se especifica con la opción **-d**) en el servidor TFTP en una dirección IP específica (que se indica con la opción **-a**). Después de que el archivo de imagen se descarga del servidor TFTP, el proceso de actualización comienza. Al terminar, el iDRAC6 se restablece.

- `racadm fwupdate -s`

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

---

krbkeytabupload

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

La Tabla A-40 describe el subcomando **krbkeytabupload**.

Tabla A-40. krbkeytabupload

Subcomando	Descripción
krbkeytabupload	Permite cargar un archivo keytab de Kerberos.

Sinopsis

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

<nombre de archivo> es el nombre del archivo que incluye la ruta de acceso.

Opciones

La Tabla A-41 describe las opciones del subcomando **krbkeytabupload**.

Tabla A-41. Opciones del subcomando krbkeytabupload

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

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

Ejemplo

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

Interfaces admitidas

- RACADM remoto
- RACADM local

---

vmkey

Sinopsis

```
racadm vmkey reset
```

Descripción

El subcomando **vmkey** restablece la partición de Virtual Flash al tamaño predeterminado de 256 MB y elimina todos los datos de la misma.

Valores legales

reset = Restablece la partición de Virtual Flash al tamaño predeterminado de 256 MB y elimina todos los datos de la misma.

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

version

Sinopsis

```
racadm version
```

Descripción

Muestra la versión de RACADM

Interfaces admitidas

- RACADM remoto
- RACADM local
- RACADM SSH/Telnet

---

arp

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

La Tabla A-42 describe el comando **arp**.

Tabla A-42. Comando arp

Comando	Definición
arp	Muestra el contenido de la tabla ARP. Los registros de la tabla ARP no se pueden agregar ni eliminar.

Sinopsis

```
racadm arp
```

Descripción

Muestra la tabla del Protocolo de resolución de direcciones (ARP).

Ejemplo

Dirección IP tipo de HW Indicadores Dirección de HW Máscara Dispositivo

192.168.1.1 0x1 0x2 00:00:0C:07:AC:0F * eth0

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

coredump

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

La Tabla A-43 describe el subcomando **coredump**.

Tabla A-43. coredump

Subcomando	Definición
coredump	Muestra el último volcado de núcleo del iDRAC6.

Sinopsis

```
racadm coredump
```

Descripción

El subcomando **coredump** muestra la información detallada que se relaciona con los problemas críticos recientes que hayan surgido con el iDRAC6. La información de volcado de núcleo se puede usar para diagnosticar estos problemas críticos.

Si está disponible, la información de volcado de núcleo permanece después de ciclos de encendido del iDRAC6 y seguirá disponible hasta que se presente alguna de las condiciones siguientes:

- La información de volcado de núcleo se borra con el subcomando **coredumpdelete**.
- Se presenta otra condición crítica en el iDRAC6. En este caso, la información de volcado de núcleo se referirá al último error crítico que se haya presentado.

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

coredumpdelete

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

La Tabla A-44 describe el subcomando **coredumpdelete**.

Tabla A-44. coredumpdelete

Subcomando	Definición
coredumpdelete	Borra el volcado de núcleo almacenado en el iDRAC6.

Sinopsis

```
racadm coredumpdelete
```

Descripción

El subcomando **coredumpdelete** se puede usar para borrar los datos de **volcado de núcleo** que residan en ese momento en el iDRAC6.

NOTA: Si se ejecuta un comando **coredumpdelete** y no hay un volcado de núcleo almacenado en el iDRAC6 en ese momento, el comando mostrará un mensaje de ejecución correcta. Este comportamiento es normal.

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

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

ifconfig

NOTA: Para usar este comando, se debe tener permiso para **Ejecutar comandos de diagnóstico** o para **Configurar el iDRAC6**.

La Tabla A-45 describe el subcomando **ifconfig**.

Tabla A-45. ifconfig

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

Sinopsis

```
racadm ifconfig
```

Ejemplo

```
$ racadm ifconfig

eth0 Link encap:Ethernet HWaddr 00:1D:09:FF:DA:23

inet addr:10.35.155.136 Bcast:10.35.155.255 Mask:255.255.255.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:2550665 errors:0 dropped:0 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:272532097 (259.9 MiB) TX bytes:0 (0.0 B)
```

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

netstat

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

La Tabla A-46 describe el subcomando **netstat**.

Tabla A-46. netstat

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

Sinopsis

```
racadm netstat
```

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

ping

NOTA: Para usar este comando, se debe tener permiso para **Ejecutar comandos de diagnóstico** o para **Configurar el iDRAC6**.

La Tabla A-47 describe el subcomando **ping**.

Tabla A-47. ping

Subcomando	Definición
ping	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se requiere una dirección IP de destino. Un paquete de eco de ICMP se envía a la dirección IP de destino en función del contenido de tabla de enrutamiento actual.

Sinopsis

```
racadm ping <dirección_IP>
```

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

ping6

NOTA: Para usar este comando, se debe tener permiso para **Ejecutar comandos de diagnóstico** o para **Configurar el iDRAC6**.

La Tabla A-48 describe el subcomando **ping6**.

Tabla A-48. ping6

Subcomando	Definición
ping6	Verifica que se pueda acceder a la dirección IPv6 de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se requiere una dirección IPv6 de destino. Un paquete de eco de ICMP se envía a la dirección IPv6 de destino en función del contenido de la tabla de enrutamiento actual.

Sinopsis

```
racadm ping6 <dirección_ipv6>
```

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

racdump

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

La Tabla A-49 describe el subcomando **racdump**.

Tabla A-49. racdump

Subcomando	Definición
racdump	Muestra información general y del estado del iDRAC6.

Sinopsis

```
racadm racdump
```

Descripción

El subcomando **racdump** proporciona un solo comando para obtener el volcado, el estado y la información general de la tarjeta del iDRAC6.

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

- Información general del sistema/RAC
- Volcado de núcleo
- Información de la sesión
- Información del proceso
- Información de la compilación de firmware

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

traceroute

NOTA: Para utilizar este comando, debe contar con permisos de **Administrador**.

La Tabla A-50 describe el subcomando **traceroute**.

Tabla A-50. traceroute

Subcomando	Definición
traceroute	Rastrea la ruta de red de enrutadores que toman los paquetes a medida que se reenvían desde el sistema hasta una dirección IPv4 de destino.

Sinopsis

```
racadm traceroute <IPv4 address>

racadm traceroute 192.168.0.1

traceroute to 192.168.0.1 (192.168.0.1), 30 hops max,

40 byte packets

1 192.168.0.1 (192.168.0.1) 0.801 ms 0.246 ms 0.253 ms
```

Descripción

Rastrea una ruta mediante IPv4 hacia un destino en la red.

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

traceroute6

NOTA: Para utilizar este comando, debe contar con permisos de **Administrador**.

La Tabla A-51 describe el subcomando **traceroute6**.

Tabla A-51. traceroute6

Subcomando	Definición
traceroute6	Rastrea la ruta de red de enrutadores que los paquetes toman a medida que se reenvían desde el sistema hasta una dirección IPv6 de destino.

Sinopsis

```
racadm traceroute6 <IPv6 address>

racadm traceroute fd01::1
```

```
traceroute to fd01::1 (fd01::1) from fd01::3, 30 hops

max, 16 byte packets

1 fd01::1 (fd01::1) 14.324 ms 0.26 ms 0.244 ms
```

Descripción

Rastrea una ruta mediante IPv6 hacia un destino en la red.

Interfaces admitidas

- RACADM remoto
- RACADM Telnet/SSH

---

remoteimage

NOTA: Para utilizar este comando, debe contar con permisos de **Administrador**.

La Tabla A-52 describe el subcomando **remoteimage**.

Tabla A-52. remoteimage

Subcomando	Definición
remoteimage	Conecta, desconecta o instala un archivo de medios en un servidor remoto.

Sinopsis

```
racadm remoteimage <opciones>
```

Las opciones son:

-c; conectar imagen

-d; desconectar imagen

-u <nombre_de_usuario>; nombre de usuario para acceder al recurso compartido de red

-p <contraseña>; contraseña para acceder al recurso compartido de red

-l <ubicación_de_imagen>; ubicación de la imagen en el recurso compartido de red; indique la ubicación entre comillas dobles

-s; mostrar el estado actual; -a se da por hecho si no se especifica

Descripción

Conecta, desconecta o instala un archivo de medios en un servidor remoto.

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

---

sshpkauth

Sinopsis

racadm sshpkauth

Cargar

El modo de carga permite cargar un archivo de clave o copiar el texto de la clave en la línea de comandos. No es posible cargar y copiar una clave al mismo tiempo.

Vista

El modo de vista le permite al usuario ver una clave que haya especificado o todas las claves.

Delete

El modo de eliminación le permite al usuario eliminar una clave que haya especificado o todas las claves.

Descripción

Permite cargar y administras hasta 4 claves públicas SSH diferentes *por usuario*. Puede cargar un archivo de claves o el texto de la clave, ver claves o eliminarlas. Este comando tiene tres modos exclusivos entre sí: cargar, ver y eliminar que están determinados por las opciones (consultar Tabla A-53) proporcionadas en el comando.

Opciones

Tabla A-53. Opciones de subcomandos sshpkauth

Opción	Descripción
-i <índice del usuario>	Índice del usuario. <índice del usuario> debe estar entre 2 y 16 en iDRAC6.
-k [<índice de claves> | all]	Índice para asignar la clave PK que se va a cargar. "**all**" únicamente funciona con las opciones -v o -d. <índice de claves> debe estar entre 1 y 4 o "**all**" en iDRAC6.
-t <Texto de la clave PK>	Texto de la clave para la clave pública SSH.
-f <nombre de archivo>	Archivo que incluye el texto de la clave que se va a cargar. La opción **-f** no se admite en el RACADM de telnet/ssh.
-v	Vea el texto de la clave del índice proporcionado.
-d	Elimine la clave del índice proporcionado.

Ejemplos

Cargue una clave inválida en usuario 2 de iDRAC6 en el primer espacio de clave por medio de una cadena:

```
$ racadm sshpkauth -i 2 -k 1 -t "Este es texto de clave inválida"

ERROR: Clave SSH inválida
```

Cargue una clave válida en el usuario 2 de iDRAC6 en el primer espacio de clave por medio de un archivo:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key

PK SSH Authentication Key file successfully uploaded to the RAC.
```

Obtenga todas las claves para el usuario 2 de iDRAC6:

```
$ racadm sshpkauth -v -i 2 -k all

******************** ID del usuario 2 ******************

Key ID 1:

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzzy+k2npnKqVEXGXIzo0sbR6JgA5YNbWs3ekoxXV
fe3yJVpVc/5zrrr7XrwKbJAJTqSw8Dg3iR4n3vUaP+lPHmUv5Mn55Ea6LHUslAXFqXmOdlThd wilU2VLw/iRH1ZymUFnut8ggbPQgqV2L8bsUaMqb5PooIIvV6hy4isCNJU= 1024-bit
RSA, converted from OpenSSH by xx_xx@xx.xx

Key ID 2:

SSH Key not available

Key ID 3:

SSH Key not available

Key ID 4:
```

```
SSH Key not available
```

Interfaces admitidas

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

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 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

La base de datos de propiedades del iDRAC6 contiene la información de configuración del iDRAC6. 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 si se indica lo contrario.

△ **PRECAUCIÓN: Ciertos grupos y objetos descritos en este capítulo no están disponibles en la versión 6.2 de Dell™ OpenManage™. Se van a admitir en la versión 6.3 de Dell OpenManage.**

Caracteres que se pueden mostrar

Los caracteres que se pueden mostrar incluyen el siguiente conjunto:

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

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

Se permite una instancia de grupo. Las siguientes subsecciones describen los objetos en este grupo.

idRacProductInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII.

Predeterminado

Integrated Dell Remote Access Controller.

Descripción

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

Descripción de texto del tipo de RAC.

idRacVersionInfo (sólo lectura)

Valores legales

Cadena de hasta 63 caracteres ASCII.

Predeterminado

Ninguno

Descripción

Cadena que contiene la versión actual del firmware del producto.

idRacBuildInfo (sólo lectura)

Valores legales

Cadena de hasta 16 caracteres ASCII.

Predeterminado

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

Descripción

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

Nombre de usuario asignado para identificar este controlador.

idRacType (sólo lectura)

Valores legales

Identificación del producto

Predeterminado

8

Descripción

Identifica el tipo de controlador de acceso remoto como iDRAC6.

---

cfgOobSnmp

Este grupo contiene parámetros para configurar las funciones de excepción y de agente SNMP del iDRAC6.

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

cfgOobSnmpAgentCommunity (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 31

Predeterminado

public

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 el NIC del iDRAC6

Se permite una instancia de grupo. Todos los objetos en este grupo requerirán que se restablezca el NIC del iDRAC6, lo que puede ocasionar una breve pérdida de conectividad. Los objetos que cambien la configuración de la dirección IP de el 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.

NOTA: Para que los cambios de propiedades de la red en el iDRAC6 se ejecuten correctamente a través de RACADM, primero debe activar el NIC del iDRAC6.

NOTA: A los objetos VLAN (cfgNicVLanEnable, cfgNicVLanId y cfgNicVLanPriority) que se muestran por medio de los comandos de RACADM local "racadm getconfig -g cfgLanNetworking" o en el archivo de configuración generado de los comandos de RACADM local "racadm getconfig -f <nombre de archivo>" les falta el símbolo principal "#" que se usa para indicar la naturaleza de sólo lectura de estos objetos.

cfgNicIPv4Enable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Activa o desactiva la pila de IPv4 del iDRAC6.

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 Por lo menos uno de los caracteres debe ser alfabético. Los caracteres se limitan a caracteres alfanuméricos, guiones y puntos.

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

Predeterminado

(en blanco)

Descripción

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. Por lo 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

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

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 (NIC) del iDRAC6. Si el NIC está desactivado, las interfaces remotas de red al iDRAC6 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

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

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

Predeterminado

255.255.255.0

Descripción

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

Cadena que representa una dirección IP de puerta de enlace válida. Por ejemplo: 192.168.0.1.

Predeterminado

192.168.0.1

Descripción

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 estática, la máscara de subred y la puerta de enlace se asignarán a partir de las propiedades **cfgNicIpAddress**, **cfgNicNetmask** y **cfgNicGateway**.

cfgNicMacAddress (sólo lectura)

Valores legales

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

Predeterminado

Dirección MAC actual del NIC del iDRAC6. Por ejemplo, 00:12:67:52:51:A3.

Descripción

Dirección MAC del NIC del iDRAC6.

cfgNicVLanEnable (sólo lectura)

NOTA: La configuración de VLAN puede definirse a través de la interfaz web del CMC. El iDRAC6 sólo muestra la configuración actual de VLAN pero no se puede modificar la configuración desde el iDRAC6.

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva las funciones de VLAN del iDRAC6 desde el CMC.

cfgNicVLanID (sólo lectura)

Valores legales

De 1 a 4094

Predeterminado

1

Descripción

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

cfgNicVLanPriority (sólo lectura)

Valores legales

De 0 a 7

Predeterminado

0

Descripción

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

---

cfgIPv6URL

Este grupo especifica las propiedades utilizadas para configurar la dirección URL IPv6 del iDRAC6.

cfgIPv6URLstring (sólo lectura)

Valores legales

Cadena de hasta 80 caracteres.

Predeterminado

<vacío>

Descripción

Dirección URL IPv6 de iDRAC6.

---

cfgIPv6LanNetworking

Este grupo se utiliza para configurar IPv6 sobre las capacidades de sistema de red de LAN

cfgIPv6Enable

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la pila de IPv6 del iDRAC6.

cfgIPv6Address1 (lectura/escritura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección IPv6 del iDRAC6.

cfgIPv6Gateway (lectura/escritura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección IPv6 de puerta de enlace del iDRAC6.

cfgIPv6PrefixLength (lectura/escritura)

Valores legales

De 1 a 128

Predeterminado

0

Descripción

Longitud del prefijo para dirección 1 IPv6 del iDRAC6.

cfgIPv6AutoConfig (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la opción AutoConfig de IPv6.

cfgIPv6LinkLocalAddress (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección local del vínculo IPv6 del iDRAC6.

cfgIPv6Address2 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección IPv6 del iDRAC6.

cfgIPv6DNSServersFromDHCP6 (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Especifica si cfgIPv6DNSServer1 y cfgIPv6DNSServer2 son direcciones IPv6 de DHCP o estáticas.

cfgIPv6DNSServer1 (lectura/escritura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección IPv6 del servidor DNS.

cfgIPv6DNSServer2 (lectura/escritura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

::

Descripción

Dirección IPv6 del servidor DNS.

cfgIPv6Address3 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address4 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address5 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address6 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address7 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address8 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address9 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address10 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address11 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address12 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address13 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address14 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

cfgIPv6Address15 (sólo lectura)

Valores legales

Cadena que representa una entrada de IPv6 válida.

Predeterminado

<vacío>

---

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

Privilegio máximo en el canal de LAN de IPMI.

cfgUserAdminPrivilege (lectura/escritura)

Valores legales

De 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 para privilegio de usuario que se pueden combinar para crear máscaras de bit.

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

Privilegio de usuario	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

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 de usuario

Privilegios de 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

Nombre de usuario para este índice. El índice de usuario se crea al escribir una cadena en el campo de este nombre si el índice está en blanco. Si escribe una cadena de comillas dobles (""), se elimina el usuario de ese índice. No se puede cambiar el nombre. Debe eliminarlo y volver a crear el nombre. La cadena no debe tener / (barras diagonales), \ (barras diagonales invertidas), . (puntos), @ (arrobas) o comillas.

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

cfgUserAdminPassword (de sólo escritura)

Valores legales

Cadena de hasta 20 caracteres ASCII.

Predeterminado

(vacío)

Descripción

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 (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva un usuario individual.

cfgUserAdminSolEnable (lectura/escritura)

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

Índice único de una instancia de alerta.

cfgEmailAlertEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

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

cfgEmailAlertAddress (lectura/escritura)

Valores legales

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

Predeterminado

(vacío)

Descripción

Dirección de correo electrónico del origen de la alerta.

cfgEmailAlertCustomMsg (lectura/escritura)

Valores legales

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 2

Predeterminado

2

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 inactiva (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 inactiva (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.

Una sesión Secure Shell que ha finalizado muestra el siguiente mensaje de error sólo después de que oprima <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.

cfgSsnMgtTelnetTimeout (lectura/escritura)

Valores legales

0 (sin tiempo de espera)

De 60 a 10800

Predeterminado

1800

Descripción

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

Cuando la sesión de Telnet expire, aparecerá el siguiente mensaje de error sólo si usted presiona <Entrar>:

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

Después de que el mensaje aparezca, el sistema regresará al shell que generó la sesión de 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 SMTP para las alertas de correo electrónico.

cfgRhostsSmtpServerIpAddr (lectura / escritura)

Valores legales

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

Predeterminado

0.0.0.0

Descripción

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

cfgRhostsFwUpdateTftpEnable (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

1

Descripción

Activa o desactiva la actualización del firmware del iDRAC6 a partir de un servidor TFTP de red.

cfgRhostsFwUpdateIpAddr (lectura/escritura)

Valores legales

Cadena que representa una dirección IP válida.

Predeterminado

0.0.0.0

Descripción

Especifica la dirección IP del servidor TFTP de red que se utiliza para operaciones de actualización del firmware del iDRAC6 por TFTP.

cfgRhostsFwUpdatePath (lectura/escritura)

Valores legales

Cadena con una longitud máxima de 255 caracteres ASCII.

Predeterminado

<vacío>

Descripción

Especifica la ruta de acceso de TFTP en la que se encuentra el archivo de imagen del firmware del iDRAC6 en el servidor TFTP. La ruta de acceso de TFTP es relativa a la ruta de acceso raíz de TFTP en el servidor TFTP.

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

cfgRhostsSyslogEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva el registro del sistema remoto.

cfgRhostsSyslogPort (lectura/escritura)

Valores legales

0 - 65535

Predeterminado

514

Descripción

Número de puerto de registro del sistema remoto.

cfgRhostsSyslogServer1 (lectura/escritura)

Valores legales

Cadena de 0 a 511 caracteres.

Predeterminado

<vacío>

Descripción

Nombre del servidor registro del sistema remoto.

cfgRhostsSyslogServer2 (lectura/escritura)

Valores legales

Cadena de 0 a 511 caracteres.

Predeterminado

<vacío>

Descripción

Nombre del servidor registro del sistema remoto.

cfgRhostsSyslogServer3 (lectura/escritura)

Valores legales

Cadena de 0 a 511 caracteres.

Predeterminado

<vacío>

Descripción

Nombre del servidor registro del sistema remoto.

---

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

1 - 40

Predeterminado

<instancia>

Descripción

Representa un dominio específico.

cfgUserDomainName (lectura/escritura)

Valores legales

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 energía.

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.**

cfgServerActualPowerConsumption (sólo lectura)

Valores legales

Cadena de hasta 32 caracteres.

Predeterminado

(vacío)

Descripción

Representa el consumo de energía del servidor en este momento.

cfgServerPeakPowerConsumption (sólo lectura)

Valores legales

Cadena de hasta 32 caracteres.

Predeterminado

(vacío)

Descripción

Representa el consumo máximo de energía del servidor hasta el momento.

cfgServerPeakPowerConsumptionTimestamp (sólo lectura)

Valores legales

Cadena de hasta 32 caracteres.

Predeterminado

(vacío)

Descripción

Hora en que se registró el consumo máximo de energía.

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

Cadena de hasta 32 caracteres.

Predeterminado

(vacío)

Descripción

Representa el umbral de alimentación del servidor en vatios.

cfgServerPowerCapBtuhr (sólo lectura)

Valores legales

Cadena de hasta 32 caracteres.

Predeterminado

(vacío)

Descripción

Representa el umbral de alimentación del servidor expresado en BTU/h.

cfgServerPowerCapPercent (sólo lectura)

Valores legales

Cadena de hasta 32 caracteres.

Predeterminado

(vacío)

Descripción

Representa el umbral de alimentación del servidor expresado en porcentajes.

---

cfgRacTuning

Este grupo se usa para configurar varias propiedades 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

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 unos 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

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

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

cfgRacTuneIpBlkFailWindow

Valores legales

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

cfgRacTuneSshPort (lectura/escritura)

Valores legales

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 mouse 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 del iDRAC6 antes de activarse.

cfgRacTuneAsrEnable (lectura / escritura)

Valores legales

0 (FALSE)

1 (TRUE)

Predeterminado

1

Descripción

Activa o desactiva la función de captura de pantalla de último bloqueo del iDRAC6.

NOTA: Este objeto requiere de un restablecimiento del 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 (Enables)

0 (Disables)

Predeterminado

1

Descripción

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

cfgRacTuneDaylightOffset (lectura/escritura)

Valores legales

De 0 a 60

Predeterminado

0

Descripción

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

cfgRacTuneTimezoneOffset (lectura/escritura)

Valores legales

De -720 a 780

Predeterminado

0

Descripción

Especifica la diferencia de zona horaria (en minutos) en relación con GMT/UTC que se utiliza para la

hora del RAC. A continuación se enumeran algunas diferencias de zona horaria para los

Estados Unidos:

-480 (PST: Hora estándar de la costa del Pacífico)

-420 (MST: Hora estándar de la zona de las montañas)

-360 (CST: Hora estándar de la región central)

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

cfgRacTuneLocalConfigDisable (lectura/escritura)

Valores legales

0 (Enables)

1 (Disables)

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 de RACADM local o la interfaz web del iDRAC6; sin embargo, una vez desactivado, 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

Cadena de hasta 255 caracteres.

Predeterminado

(vacío)

Descripción

Nombre de host del servidor administrado.

ifcRacMnOsOsName (sólo lectura)

Valores legales

Cadena de hasta 255 caracteres.

Predeterminado

(vacío)

Descripción

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** de RACADM para obtener más información sobre cómo generar solicitudes de firma de certificado.

cfgSecCsrCommonName (lectura/escritura)

Valores legales

Cadena de hasta 254 caracteres ASCII.

Predeterminado

Descripción

Especifica el nombre común (CN) de la CSR.

cfgSecCsrOrganizationName (lectura/escritura)

Valores legales

Cadena de hasta 254 caracteres ASCII.

Predeterminado

(vacío)

Descripción

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

cfgSecCsrOrganizationUnit (lectura/escritura)

Valores legales

Cadena de hasta 254 caracteres ASCII.

Predeterminado

(vacío)

Descripción

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

cfgSecCsrLocalityName (lectura/escritura)

Valores legales

Cadena de hasta 254 caracteres ASCII.

Predeterminado

(vacío)

Descripción

Especifica la localidad (L) de la CSR.

cfgSecCsrStateName (lectura/escritura)

Valores legales

Cadena de hasta 254 caracteres ASCII.

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 del país (CC) de la CSR

cfgSecCsrEmailAddr (lectura/escritura)

Valores legales

Cadena de hasta 254 caracteres ASCII.

Predeterminado

(vacío)

Descripción

Especifica la dirección de correo electrónico de la 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.

cfgRacVirMediaAttached (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 válidos conectados al sistema. Esto equivale a conectar una unidad USB de CD-ROM/unidad de disco flexible local a un puerto USB del sistema. Cuando los dispositivos estén conectados, es posible conectarse a los dispositivos virtuales de manera remota utilizando 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.

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 memoria del medio VFlash del iDRAC6.

cfgVirtualFloppyEmulation (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:.

cfgSDWriteProtect (sólo lectura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

---

cfgIpmiLan

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

cfgIpmiLanEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

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

1 (TRUE)

0 (FALSE)

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 un número par de dígitos hexadecimales de 0 a 40 caracteres sin espacios.

Predeterminado

0000000000000000000000000000000000000000

Descripción

Clave de cifrado de IPMI.

cfgIpmiPetCommunityName (lectura/escritura)

Valores legales

Una cadena de hasta 18 caracteres.

Predeterminado

public

Descripción

Nombre de comunidad SNMP para las capturas.

---

cfgIpmiPetIpv6

Este grupo se usa para configurar las capturas de sucesos de plataforma IPv6 en el servidor administrado.

cfgIpmiPetIPv6Index (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

<Valor de índice>

Descripción

Identificador único para el índice que corresponde a la captura.

cfgIpmiPetIPv6AlertDestIpAddr

Valores legales

Cadena que representa una dirección IPv6 válida.

Predeterminado

<vacío>

Descripción

Configura la dirección IP de destino de alerta de IPv6 para la captura.

cfgIpmiPetIPv6AlertEnable (lectura/escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva el destino de alerta IPv6 para la captura.

---

cfgIpmiPef

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

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

cfgIpmiPefName (sólo lectura)

Valores legales

Cadena de hasta 255 caracteres.

Predeterminado

Nombre del filtro de índice.

Descripción

Especifica el nombre del filtro de sucesos de plataforma.

cfgIpmiPefIndex (lectura/escritura)

Valores legales

De 1 a 9

Predeterminado

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

1 (TRUE)

0 (FALSE)

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 (sólo lectura)

Valores legales

De 1 a 4

Predeterminado

Valor de índice de una captura de suceso de plataforma específica.

Descripción

Identificador único para el índice que corresponde a la captura.

cfgIpmiPetAlertDestIpAddr (lectura/escritura)

Valores legales

Una cadena que representa una dirección IPv4 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

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva una captura específica.

---

cfgSmartCard

Este grupo especifica las propiedades utilizadas para respaldar el acceso al iDRAC6 mediante una tarjeta inteligente.

cfgSmartCardLogonEnable (lectura/escritura)

Valores legales

0 (Disabled)

1 (Enabled)

Predeterminado

0

Descripción

Activa o desactiva la compatibilidad con el acceso al iDRAC6 mediante una tarjeta inteligente.

---

cfgActiveDirectory

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

cfgADSSOEnable (lectura / escritura)

Valores legales

1 (TRUE)

0 (FALSE)

Predeterminado

0

Descripción

Activa o desactiva la autentificación de inicio de sesión único de Active Directory en el iDRAC6.

cfgADRacDomain (lectura / escritura)

Valores legales

Cualquier cadena de texto imprimible sin espacios. El número máximo de caracteres es 254.

Predeterminado

(vacío)

Descripción

Dominio de Active Directory donde reside el DRAC.

cfgADRacName (lectura / escritura)

Valores legales

Cualquier cadena de texto imprimible sin espacios. El número máximo de caracteres es 254.

Predeterminado

(vacío)

Descripción

Nombre del iDRAC6, según 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 autentificación 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). El número máximo de caracteres es 254.

Predeterminado

Ningún valor predeterminado

Descripción

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

cfgADDomainController2 (lectura/escritura)

Valores legales

Dirección IP válida o un nombre de dominio completo (FQDN). El número máximo de caracteres es 254.

Predeterminado

Ningún valor predeterminado.

Descripción

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

cfgADDomainController3 (lectura/escritura)

Valores legales

Dirección IP válida o un nombre de dominio completo (FQDN). El número máximo de caracteres es 254.

Predeterminado

Ningún valor predeterminado.

Descripción

El iDRAC6 utiliza el valor que se 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). El número máximo de caracteres es 254.

Predeterminado

Ningún valor predeterminado.

Descripción

El iDRAC6 usa el valor que se especifique 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). El número máximo de caracteres es 254.

Predeterminado

Ningún valor predeterminado.

Descripción

El iDRAC6 usa el valor que se especifique 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). El número máximo de caracteres es 254.

Predeterminado

Ningún valor predeterminado.

Descripción

El iDRAC6 usa el valor que se especifique 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

<vacío>

Descripción

Activa o desactiva la validación de certificados de Active Directory.

cfgADDcSRVLookupEnable (lectura/escritura)

Valores legales

1 (TRUE): Usa el DNS para buscar controladores de dominio

0 (FALSE): Usa controladores de dominio preconfigurados

Predeterminado

0

Definición

Configura el iDRAC6 para usar controladores de dominio preconfigurados o para usar el DNS para encontrar el controlador de dominio. Si se usan controladores de dominio preconfigurados, los controladores de dominio que hay que utilizar están especificados en cfgAdDomainController1, cfgAdDomainController2 y cfgAdDomainController3. iDRAC6 no cuenta con protección contra fallas para los controladores de dominio especificados cuando falla la búsqueda en el DNS, pues de ser así ninguno de los servidores que ofrece la búsqueda en el DNS funciona.

cfgADDcSRVLookupbyUserdomain (lectura/escritura)

Valores legales

1 (TRUE): Usa el dominio de usuario como el dominio de búsqueda para buscar los controladores de dominio. El dominio de usuario es seleccionado de la lista de dominios de usuarios o es ingresado por el usuario.

0 (FALSE): Usa el dominio de búsqueda configurado *cfgADDcSrvLookupDomainName* para buscar los controladores de dominio.

Predeterminado

1

Ejemplo

Si existe una "userid" del usuario que tiene un dominio de Active Directory "MyDomain", entonces:

Si esta opción está activada, el usuario deberá escribir "MyDomain/userid" en el campo usuario al iniciar sesión. Si esta opción está desactivada, el nombre de dominio de búsqueda cfgADDcSRVLookupDomainName debe estar configurado de forma tal que incluya el valor "MyDomain". El usuario deberá escribir su "userid" en el campo usuario al iniciar sesión.

Definición

Selecciona la forma de búsqueda del dominio de usuario de Active Directory.

cfgADDcSRVLookupDomainName (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

Nulo

Definición

Éste es el dominio de Active Directory que hay que utilizar cuando *cfgAddcSrvLookupbyUserDomain* está configurado en 0.

cfgADGcSRVLookupEnable (lectura/escritura)

Valores legales

0(FALSE): Usa servidores de Catálogo global (GCS) preconfigurados

1(TRUE): Usa el DNS para buscar servidores de catálogo global

Predeterminado

0

Definición

Determina la forma de búsqueda del servidor de catálogo global. Si se usan servidores de catálogo global preconfigurados, entonces el iDRAC6 usa los valores cfgAdGlobalCatalog1, cfgAdGlobalCatalog2 y cfgAdGlobalCatalog3.

cfgADGcRootDomain (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

Nulo

Ejemplo

Si su dominio es "ROOTDOMAIN.sub1", entonces este valor se configura como "ROOTDOMAIN" (dominio raíz).

Descripción

El nombre del dominio raíz de Active Directory utilizado para buscar el DNS y ubicar los servidores de catálogo global.

---

cfgLDAP

Este grupo permite configurar los valores relacionados con el Protocolo ligero de acceso a directorios (LDAP).

cfgLdapEnable (lectura/escritura)

Valores legales

1 (TRUE): Activa los servicios de LDAP

0 (FALSE): Desactiva los servicios de LDAP

Predeterminado

0

Descripción

Enciende o apaga los servicios de LDAP.

cfgLdapServer (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 1024

Predeterminado

Nulo

Descripción

Configura la dirección del servidor LDAP.

cfgLdapPort (lectura/escritura)

Valores legales

De 1 a 65535

Predeterminado

636

Descripción

Puerto de LDAP a través de SSL. No se admiten puertos que no sean SSL.

cfgLdapBasedn (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

Nulo

Descripción

El nombre de dominio de la rama del directorio donde deben iniciarse todas las búsquedas.

cfgLdapUserAttribute (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

Nulo

uid si no está configurado.

Descripción

Especifica el atributo de usuario que hay que buscar. Si no está configurado, el valor predeterminado que se utiliza es *uid*. Se recomienda que sea único dentro del DN de base seleccionado, pues de lo contrario será necesario configurar un filtro de búsqueda para garantizar la singularidad del usuario. Si el DN del usuario no puede ser identificado de forma exclusiva, el inicio de sesión falla con un error.

cfgLdapGroupAttribute (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

Nulo

Descripción

Especifica qué atributo de LDAP se utiliza para verificar la membresía del grupo. Éste deberá ser un atributo de la clase de grupos. Si no está especificado, iDRAC6 usa los atributos de *miembro* y *miembro único*.

cfgLdapGroupAttributeIsDN (lectura/escritura)

Valores legales

1 (TRUE): Usa el *DN de usuario* del servidor LDAP

0 (FALSE): Usa el *DN de usuario* proporcionado por el usuario

Predeterminado

1

Descripción

Cuando está configurado en 1, iDRAC6 compara el DN de usuario recuperado del directorio para compararlo con los miembros del grupo; si está configurado en 0, se usa el nombre de usuario proporcionado por el usuario para compararlo con los miembros del grupo. Esto no afecta al algoritmo de búsqueda del enlace. iDRAC6 siempre busca el *DN de usuario* y usa el *DN de usuario* para establecer un enlace.

cfgLdapBinddn (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

Nulo

Descripción

Nombre distintivo de un usuario que se utiliza para establecer un enlace con el servidor cuando busca el DN de usuario de inicio de sesión. Si no se indica, se utiliza un enlace anónimo. Este es opcional, pero se requiere si no admite el enlace anónimo.

cfgLdapBindpassword (sólo escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

Nulo

Descripción

Contraseña de enlace para usar junto con el DN de enlace. La contraseña de enlace es información confidencial, por lo que debe estar protegida correctamente. Es opcional, pero se requiere si no admite el enlace anónimo.

cfgLdapSearchFilter (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 254

Predeterminado

(objectclass=*)

Busca todos los objetos en el árbol.

Descripción

Filtro de búsqueda de LDAP válido. Se utiliza cuando el atributo del usuario no puede identificar de forma exclusiva al usuario dentro del *DN de base* seleccionado. El "filtro de búsqueda" sólo se aplica para la búsqueda del *DN de usuario* y no para la búsqueda de pertenencia a grupo.

cfgLDAPCertValidationEnable (lectura/escritura)

Valores legales

1 (TRUE): iDRAC6 usa el certificado de CA para validar el certificado del servidor LDAP durante el protocolo de enlace de SSL

0 (FALSE): iDRAC6 omite el paso de validación de certificados del protocolo de enlace de SSL

Predeterminado

1: Activado

Descripción

Controla la validación de certificados durante el protocolo de enlace de SSL.

---

cfgLdapRoleGroup

Este grupo permite al usuario configurar grupos de funciones para LDAP. Este grupo está indexado del 1 al 5.

cfgLdapRoleGroupIndex (sólo lectura)

Valores legales

Número entero entre 1 y 5.

Predeterminado

<instancia>

Descripción

Éste es el valor de índice del objeto de grupo de funciones.

cfgLdapRoleGroupDN (lectura/escritura)

Valores legales

Cadena. Longitud máxima = 1024

Predeterminado

Nulo

Descripción

Nombre de dominio del grupo en el índice.

cfgLdapRoleGroupPrivilege (lectura/escritura)

Valores legales

0x00000000 a 0x000001ff

Predeterminado

0x000

Descripción

Máscara de bits que define los privilegios asociados con este grupo en particular.

---

cfgStandardSchema

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

cfgSSADRoleGroupIndex (sólo lectura)

Valores legales

1 a 5

Descripción

Índice del grupo de funciones según 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 según está registrado en 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

Dominio de Active Directory donde reside el grupo de funciones.

cfgSSADRoleGroupPrivilege (lectura/escritura)

Valores legales

0x00000000 a **0x000001ff**

Predeterminado

<vacío>

Descripción

Utilice los números de máscara de bits de la Tabla B-3 para establecer los privilegios de autoridad con base en 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

Velocidad en baudios de la comunicación serie en la LAN.

cfgIpmiSolMinPrivilege (lectura/escritura)

Valores legales

2 (Usuario)

3 (Operador)

4 (Administrador)

Predeterminado

4

Descripción

Especifica el nivel de privilegio mínimo necesario para el acceso de comunicación 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

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.

Regresar a la página de contenido

Regresar a la página de contenido

Descripción general del iDRAC6 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Integrated Dell™ Remote Access Controller (iDRAC6) Enterprise es una solución de hardware y software de administración de sistemas que permite 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 remoto de control y supervisión, y coexiste en la placa base con el servidor Dell PowerEdge administrado. El sistema operativo del servidor ejecuta programas de aplicación; iDRAC6 supervisa y administra el entorno y el estado del servidor fuera del sistema operativo.

Se puede configurar el iDRAC6 para que éste 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 de un bloqueo de sistema, iDRAC6 puede registrar datos de eventos 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. Cada módulo de alta densidad en un chasis tiene un iDRAC6. Es posible instalar un total de 16 módulos de alta densidad en el M1000e.

Todas las conexiones de red al iDRAC6 se enrutan a través de las interfaces de red del CMC (el puerto de conexión RJ45 del CMC etiquetado "GB1"). El CMC enruta el tráfico hacia los dispositivos iDRAC6 a través 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, está *fuera de banda*. Se puede acceder a las interfaces de red *dentro de banda* del servidor administrado mediante los módulos de E/S (IOM) instalados en el chasis.

NOTA: Se recomienda aislar o separar la red de administración del chasis, que es usada por el iDRAC6 y el CMC, de las redes de producción. Si se mezcla el tráfico de red de administración con el de producción o aplicación, existe la posibilidad de que la red se congestione o se sature, lo que puede causar demoras de comunicación del CMC y el iDRAC6. Las demoras pueden ocasionar un comportamiento impredecible del chasis, por ejemplo, que el CMC muestre que el iDRAC6 está fuera de línea a pesar de que funciona correctamente. Esto puede ocasionar un nuevo comportamiento impredecible.

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 él a través de la dirección IP asignada 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).

Certificación IPv6 Ready Logo

La misión del Comité de IPv6 Ready Logo es definir las especificaciones de prueba de cumplimiento e interoperabilidad de IPv6 para brindar acceso a herramientas de autoprueba y ofrecer IPv6 Ready Logo.

iDRAC6 cuenta con certificación **Fase 2 de IPv6 Ready Logo** y la identificación del logotipo es **02-C-000380**. Para obtener más información sobre el programa IPv6 Ready Logo, consulte **http://www.ipv6ready.org/**.

Características de seguridad del iDRAC6

- Autentificación de usuarios por medio de Microsoft Active Directory, servicio de directorio de LDAP genérico o identificaciones y contraseñas administradas a nivel local
- Autentificación de dos factores proporcionada por la función de inicio de sesión con tarjeta inteligente. La autentificación de dos factores se basa en lo que los usuarios *tienen* (tarjeta inteligente) y lo que *conocen* (PIN)
- Autorización en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario
- Configuración de la identificación y contraseña del usuario
- Las interfaces web y SM-CLP que son compatibles con los cifrados de 128 bits y 40 bits (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)
- Puertos IP que se pueden configurar (en los casos correspondientes)
- 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 se ha superado el límite
- Rango configurable de direcciones IP para clientes que se conectan al iDRAC6

---

iDRAC6 Enterprise y tarjeta del medio VFlash

iDRAC6 Enterprise incluye una ranura SD para tarjetas de los medios VFlash. Para obtener más información acerca del iDRAC6 Enterprise y la tarjeta del medio VFlash, consulte el *Manual del propietario del hardware* en **support.dell.com / manuals**.

La Tabla 1-1 enumera las funciones disponibles para iDRAC6 Enterprise y la tarjeta del medio VFlash.

Tabla 1-1. Lista de funciones del iDRAC6

Componente	iDRAC6 Enterprise	iDRAC6 Enterprise con tarjeta del medio VFlash
Compatibilidad con interfaces y estándares		
IPMI 2.0	✓	✓
Interfaz para el usuario de web	✓	✓
SNMP	✓	✓
WS-MAN	✓	✓
SM-CLP	✓	✓
Línea de comandos RACADM	✓	✓
Conectividad		
Modos de red compartida y de recuperación ante fallas	✓	✓
IPv4	✓	✓
Etiquetado VLAN	✓	✓
IPv6	✓	✓
DNS dinámico	✓	✓
NIC dedicado	✓	✓
Seguridad y autenticación		
Autorización basada en funciones	✓	✓
Usuarios locales	✓	✓
Active Directory	✓	✓
Autenticación de dos factores	✓	✓
Inicio de sesión único	✓	✓
Cifrado SSL	✓	✓
Corrección y administración remota		
Actualización remota de firmware	✓	✓
Control de alimentación de servidor	✓	✓
Comunicación en serie en la LAN (con proxy)	✓	✓
Comunicación en serie en la LAN (sin proxy)	✓	✓
Límites de alimentación	✓	✓
Captura de pantalla de último bloqueo	✓	✓
Captura de inicio	✓	✓
Medios virtuales	✓	✓
Uso compartido de archivos remotos	✓	✓
Consola virtual	✓	✓
Consola virtual compartida	✓	✓
vFlash	✗	✓
Supervisión		
Alerta y supervisión de sensor	✓	✓
Supervisión de alimentación en tiempo real	✓	✓
Gráficos de alimentación en tiempo real	✓	✓
Medidores de datos históricos de alimentación	✓	✓

Registro		
Registro de sucesos del sistema (SEL)	✓	✓
Registro del RAC.	✓	✓
Registro de rastreo	✓	✓
Registro del sistema remoto	✓	✓
✓ = compatible; ✗ = no compatible		

Plataformas compatibles

Para conocer las plataformas compatibles más recientes, consulte el archivo léame del iDRAC6 y la *Matriz de compatibilidad de software de sistemas Dell* disponible en **support.dell.com / manuals**.

Sistemas operativos admitidos

Para obtener la información más actualizada, consulte el archivo Readme del iDRAC6 y la *Matriz de compatibilidad de software de sistemas Dell* que se encuentra disponible en **support.dell.com / manuals**.

Exploradores web admitidos

Para obtener la información más actualizada, consulte el archivo Readme del iDRAC6 y la *Matriz de compatibilidad de software de sistemas Dell* que se encuentra disponible en **support.dell.com / manuals**.

NOTA: La compatibilidad con SSL 2.0 se interrumpió debido a defectos de seguridad. Asegúrese de que su explorador esté configurado para activar SSL 3.0.

Conexiones de acceso remoto admitidas

La Tabla 1-2 muestra una lista de las funciones de conexión.

Tabla 1-2. Conexiones de acceso remoto admitidas

Conexión	Funciones
Tarjeta de interfaz de red del iDRAC6	• Ethernet de 10 Mbps/100 Mbps/1 Gbps a través del puerto Gb Ethernet del CMC. • Compatibilidad con DHCP. • Notificación de sucesos por correo electrónico y capturas SNMP. • Los comandos de RACADM y shell de SM-CLP para operaciones como configuración del iDRAC6, los comandos de inicio, restablecimiento, encendido y apagado del sistema son admitidos a través de SSH y Telnet. • Compatibilidad para las utilidades de IPMI, como IPMItool e ipmish.

Puertos del iDRAC6

La Tabla 1-3 muestra una lista de los puertos en los que el iDRAC6 detecta las conexiones. La Tabla 1-4 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.

PRECAUCIÓN: iDRAC6 no verifica si hay conflictos entre los puertos configurables. Al establecer las configuraciones de los puertos, verifique que las asignaciones de puertos no entren en conflicto unas con otras.

Tabla 1-3. 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
3670, 3671	Servicio seguro de medios virtuales
5900*	Teclado y mouse de la redirección de consola
5901*	Vídeo de la redirección de consola
5988*	Utilizado para WSMAN
* Puerto configurable	

Tabla 1-4. 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 *Matriz de compatibilidad de software de sistemas Dell* proporciona información sobre los diversos sistemas Dell, los sistemas operativos admitidos por estos sistemas y los componentes de Dell OpenManage™ que se pueden instalar en estos sistemas.
- La *Guía de instalación de Dell OpenManage Server Administrator* contiene instrucciones para ayudarlo a instalar Dell OpenManage Server Administrator.
- La *Guía de instalación de Dell OpenManage Management Station Software* contiene instrucciones para ayudarlo a instalar este software, lo que incluye la utilidad de administración de la placa base, herramientas de DRAC y la utilidad de complemento de Active Directory.
- La *Guía del usuario de Dell Chassis Management Controller* y la *Guía de referencia del administrador de Dell Chassis Management Controller* proporcionan información sobre el uso del controlador que administra todos los módulos en el chasis que contiene el servidor Dell PowerEdge.
- La *Guía del usuario de Dell OpenManage IT Assistant* contiene información sobre cómo usar IT Assistant.
- La *Guía del usuario de Dell Management Console* ofrece información sobre el uso de Dell Management Console.
- 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 los paquetes Dell Update Packages como parte de su estrategia de actualización del sistema.
- La *Guía del usuario de Dell Lifecycle Controller* brinda información acerca de Unified Server Configurator (USC), Unified Server Configurator - Lifecycle Controller Enabled (USC - LCE) y servicios remotos.
- Los documentos *Asignación de elementos CIM de iDRAC6* y *Base de datos de propiedades del iDRAC6 SM-CLP*, disponibles en el Centro tecnológico empresarial de Dell (Dell Enterprise Technology Center) en **www.delltechcenter.com**, brindan información sobre la base de datos de propiedades del iDRAC6 SM-CLP, la asignación entre clases WS-MAN y destinos SM-CLP y los detalles de implementación de Dell.

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 características, 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.

Para obtener información acerca de los términos utilizados en este documento, consulte el *Glosario* disponible en el sitio web de asistencia de Dell en **support.dell.com/manuals**.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de iDRAC6 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

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 de Dell 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

Para obtener más información, consulte la *Guía de instalación de Dell OpenManage Server Administrator* y la *Guía de instalación de Dell OpenManage Management Station Software* disponibles en el sitio web de asistencia de Dell en **support.dell.com / manuals**.

Interfaces para configurar el iDRAC6

Puede configurar el iDRAC6 mediante la utilidad de configuración del iDRAC6, la interfaz web del iDRAC6, la interfaz web de Chassis Management Controller (CMC), el panel LCD del chasis, la interfaz de línea de comandos de RACADM local o remoto, iVMCLI o la interfaz de línea de comandos 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 del iDRAC6 a través de la utilidad de configuración del iDRAC6 o la interfaz de línea de comandos de RACADM local puede desactivarse mediante un comando de RACADM (consulte "Generalidades de los subcomandos de 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
Configuración del iDRAC6 Utilidad	Se accede a la utilidad de configuración del iDRAC6 al momento del inicio, y es una herramienta útil cuando se instala un nuevo servidor Dell 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 un explorador y que se puede usar para administrar el iDRAC6 de manera interactiva y supervisar el 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, actualizar el firmware del iDRAC6, establecer la configuración de la red del iDRAC6, iniciar sesión en la interfaz web del 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 y remoto	La interfaz de línea de comandos de RACADM local se ejecuta en el servidor administrado. Se accede a ella a través del iKVM o de una sesión de redirección de consola iniciada desde la interfaz web del iDRAC6. RACADM se instala en el servidor administrado cuando usted instala Dell OpenManage Server Administrator. RACADM remoto es una utilidad cliente que se ejecuta en una estación de administración. Usa una interfaz de red fuera de banda para ejecutar comandos de RACADM en el servidor administrado. La opción **-r** ejecuta el comando de RACADM en una red. Los comandos de RACADM proporcionan acceso a casi todas las funciones de iDRAC6. Usted puede inspeccionar datos de sensor, anotaciones del registro de sucesos del 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 (iVMCLI) 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 iniciando sesión en el iDRAC6 a través de Telnet o SSH y escribiendo `smclp` en la petición de la interfaz de línea de comandos. 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 comandos 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.
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 específicas (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 acceder 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 Dell 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 del iDRAC6

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

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

NOTA: Si cambia la configuración de la red del 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 sólo para permitir que el DHCP configure la red del iDRAC6.

- 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 local y remoto: 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.

NOTA: **<**, **>** y **** no se admiten para nombres de usuarios o contraseñas.

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

NOTA: Al usar el iDRAC6 en un entorno de servicio de directorios de Active Directory / LDAP genérico, asegúrese de que los nombres de los usuarios cumplan con la convención vigente del servicio de directorios de Active Directory / LDAP genérico.

Configurar servicios de directorios

Además de los usuarios locales de iDRAC6, puede usar Microsoft® Active Directory® o el servicio de directorios de LDAP genérico para autentificar los inicios de sesión de los usuarios de iDRAC6.

Para obtener más información, consulte"Uso del servicio de directorio de iDRAC6".

Configurar la filtración 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 del filtrado de IP y bloqueo de IP"
- RACADM: consulte "Configuración del filtro de IP (Rango de IP)" 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 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 sucesos 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 del 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 obtener información sobre comandos de RACADM, 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 servicio.

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

Configurar la capa de sockets seguros (SSL)

Configurar SSL para el servidor web del iDRAC6.

- Interfaz Web del iDRAC6: Consulte "Capa de sockets seguros (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 Dell 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 del medio VFlash

Instalar y configurar una tarjeta del medio VFlash para utilizarla con iDRAC6.

- Interfaz Web del iDRAC6: Consulte "Configuración de una tarjeta del medio VFlash para utilizar con el iDRAC6"

Instalación del software de servidor administrado

Instale el sistema operativo en el servidor Dell PowerEdge mediante los medios virtuales y luego instale el software Dell OpenManage en el servidor Dell 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 del chasis para definir la configuración de red de iDRAC6 desde CMC.

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

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

Iniciar la interfaz web del iDRAC6 desde el 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 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 interfaz gráfica para usuario del iDRAC6** 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 interfaz gráfica de usuario del iDRAC6.**

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 del CMC con **Server Administrator** configurado en **Privilegios de usuario** se conecta automáticamente con la interfaz web del iDRAC6 mediante el inicio de sesión único. Después de iniciar sesión, se otorgan privilegios de administrador del iDRAC6 al usuario. Esto sucede aunque éste 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 **Privilegios de usuario** pero con la misma cuenta en iDRAC6, se conecta automáticamente con iDRAC6 mediante inicio de sesión único. Una vez conectado a la interfaz web del iDRAC6, se otorgan a este usuario privilegios creados para la cuenta iDRAC6.

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

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

NOTA: En este caso, el sistema puede solicitar a los usuarios que inicien sesión 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 interfaz gráfica para usuario del iDRAC6** puede aparecer una pantalla de error.

Configuración de la conexión de red de iDRAC6

1. Haga clic en **Sistema**→ **Acceso Remoto**→ **iDRAC6.**
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 de marcación **Activar comunicación en serie en la LAN**. También puede cambiar la configuración de **Velocidad en baudios** y **Límite de nivel de privilegio del canal**.

   c. Haga clic en **Aplicar**.

   Para activar o desactivar IPMI en la LAN:

   a. Haga clic en **Red**.

      Aparece la pantalla **Red**.

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

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

   d. Haga clic en **Aplicar**.

   Para activar o desactivar DHCP:

   a. Haga clic en **Red**.

      Aparece la pantalla **Red**.

   b. Seleccione la casilla **Activar DHCP** en la sección **Configuración de IPv4** y luego en **Activar configuración automática** en la sección **Configuración de IPv6** para activar DHCP. Para utilizar el DHCP para obtener direcciones de servidor DNS, seleccione la casilla de marcación **Usar el 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 mezzanine FlexAdress

El M1000e incluye FlexAdress, un sistema de red multiestándar avanzado de varios niveles. 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 mezzanine para cada conexión de puerto y de red Fabric.

La configuración de la función FlexAddress se realiza usando la interfaz web de CMC. Para obtener más información sobre la función FlexAddress y su configuración, consulte la *Guía del usuario de Dell Chassis Management Controller* y el documento *Especificaciones técnicas de la tarjeta Secure Digital (SD) de Chassis Management Controller (CMC)*.

Una vez que la función FlexAddress se ha activado y configurado para el chasis, haga clic en **Sistema**→ ficha **Propiedades**→ **WWN/MAC** para ver una lista de las tarjetas mezzanine instaladas, las redes Fabric a las que están conectadas, el tipo de red Fabric y las direcciones MAC asignadas por el servidor o chasis para cada puerto de tarjeta mezzanine opcional y Ethernet incorporado que se haya instalado.

La columna **Asignadas por el servidor** muestra las direcciones WWN/MAC asignadas por el servidor que están integradas al hardware del controlador. Las direcciones WWN/MAC que muestran el texto **N/A** indican que no se ha instalado una interfaz para la red Fabric especificada.

La columna **Asignadas por el chasis** muestra las direcciones WWN/MAC asignadas por el chasis que se utilizan para una ranura en particular. Las direcciones WWN/MAC que muestran el texto **N/A** indican que no se ha instalado la función FlexAddress. Una marca de verificación de color verde en las columnas **Asignadas por el servidor** y **Asignadas por el chasis** indica las direcciones activas.

Dirección MAC de FlexAddress para iDRAC6

La función FlexAddress reemplaza las direcciones MAC asignadas por el servidor por direcciones MAC asignadas por el chasis y se implementa para el iDRAC junto con LOM de módulos de alta densidad, tarjetas mezzanine y módulos de E/S. La función FlexAddress del iDRAC6 admite la preservación de la dirección MAC específica de una ranura para los iDRAC6 en un chasis. La dirección MAC asignada por el chasis se almacena en la memoria no volátil y se envía al iDRAC6 durante su proceso de inicio o al cambiar la configuración en la página C MC FlexAddress.

Si el CMC activa la dirección MAC asignada por el chasis, el iDRAC6 mostrará el valor en el campo **Dirección MAC** en las siguientes pantallas:

- **Sistema→** ficha **Propiedades→ Detalles del sistema→ Información del iDRAC6**
- **Sistema→** ficha **Propiedades→ WWN/MAC**
- **Sistema→ Acceso remoto→ iDRAC6→** ficha **Propiedades→ Información de acceso remoto→ Configuración de la red**
- **Sistema→ Acceso remoto→ iDRAC6→** ficha **Red/Seguridad→ Red→ Configuración de tarjeta de interfaz de red**

PRECAUCIÓN: Con la función FlexAddress activada, si se pasa de una dirección MAC asignada por el servidor a una asignada por el chasis y viceversa, la dirección IP del iDRAC6 también cambia.

NOTA: La función FlexAddress sólo puede activarse o desactivarse a través del CMC. La interfaz gráfica para el usuario del iDRAC6 sólo muestra el estado. Toda sesión de vKVM o vMedia finalizará si se modifica la configuración de FlexAddress en la página CMC FlexAddress.

Activación de FlexAddress a través de RACADM

No se puede activar la función FlexAddress desde el iDRAC6. Active la función FlexAddress en los niveles de red fabric y ranura del CMC.

1. Desde la consola de CMC, active la función FlexAddress para el servidor administrado en la ranura con el siguiente comando de RACADM:

   `racadm setflexaddr -i <n°_de_ranura> 1`, donde <ranura_n°> es el número de ranura en el cual se puede activar la función FlexAddress.

2. Siguiente, desde la consola de CMC, active la función FlexAddress a nivel de red fabric ejecutando el siguiente comando de RACADM:

   `racadm setflexaddr -f <nombre_red fabric> 1`, donde `<nombre_red fabric>` es A, B o C.

3. Para activar la función FlexAddress para todos los iDRAC6s en el chasis, desde la consola de CMC, ejecute el siguiente comando de RACADM:

   ```
   racadm setflexaddr -f idrac 1
   ```

Consulte la *Guía de referencia del administrador de Dell Chassis Management Controller* para obtener más información acerca de los subcomandos de RACADM del CMC.

Registro del sistema remoto

La función de registro del sistema remoto del iDRAC6 permite escribir de manera remota el registro del RAC y el registro de sucesos del sistema (SEL) en un servidor de registro del sistema externo. Puede leer todos los registros del conjunto completo de servidores desde un registro central.

El protocolo de registro del sistema remoto no necesita ningún tipo de autentificación de usuario. Para que los registros ingresen al servidor registro del sistema remoto, asegúrese de que la conectividad de red entre el iDRAC6 y el servidor de registro del sistema remoto sea correcta y de que el servidor de registro del sistema remoto se ejecute en la misma red que el iDRAC6. Las anotaciones del registro del sistema remoto son paquetes UDP que se envían al puerto de registro del sistema del servidor de registro del sistema remoto. Si se producen errores en la red, el iDRAC6 no vuelve a enviar el mismo registro. El registro remoto ocurre en tiempo real a medida que los registros ingresan al registro SEL y al registro del RAC del iDRAC6. También puede cambiar la configuración de registro del sistema remoto del iDRAC6 a través del CMC.

Es posible activar registro del sistema remoto desde la interfaz web remota:

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→** ficha **Configuración→ Configuración del registro del sistema remoto**. Aparece la pantalla **Configuración del registro del sistema remoto**.

La Tabla 2-2 indica la configuración del registro del sistema remoto.

Tabla 2-2. Configuración del registro del sistema remoto

Atributo	Descripción
Registro del sistema remoto activado	Seleccione esta opción para activar la transmisión y captura remota de registro del sistema en el servidor especificado. Una vez activado registro del sistema, se envían nuevas anotaciones de registro a los servidores registro del sistema.
Servidor registro del sistema 1-3	Introduzca la dirección del servidor registro del sistema remoto para registrar mensajes del iDRAC6 como registros SEL y del RAC. Las direcciones de servidores registro del sistema admiten caracteres alfanuméricos y los símbolos -, ., : y _.
Número de puerto	Introduzca el número de puerto del servidor registro del sistema remoto. El número de puerto debe estar entre 1 y 65535. El predeterminado es 514.

NOTA: Los niveles de gravedad que define el protocolo de registro del sistema remoto difieren de los del registro de sucesos del sistema (SEL) de IPMI estándar. En consecuencia, todas las anotaciones de registro del sistema remoto del iDRAC6 se informan al servidor registro del sistema con niveles de gravedad de **Aviso**.

El siguiente ejemplo muestra los objetos de configuración y el uso del comando de RACADM para cambiar la configuración de registro del sistema remoto:

```
racadm config –g cfgRemoteHosts –o cfgRhostsSyslogEnable [1/0]; el valor predeterminado es 0

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogServer1 <nombre_del_servidor_1>; el valor predeterminado es en blanco

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogServer2 <nombre_del_servidor_2>; el valor predeterminado es en blanco

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogServer3 <nombre_del_servidor_3>; el valor predeterminado es en blanco

racadm config –g cfgRemoteHosts –o cfgRhostsSyslogPort <número_de_puerto>; el valor predeterminado es 514
```

Uso compartido de archivos remotos

La función de uso compartido de archivos remotos a través del iDRAC6 permite especificar un archivo de imagen ISO de CD/DVD ubicado en un recurso compartido de red y ponerlo a disposición del sistema operativo del servidor como unidad virtual montándolo como CD o DVD mediante NFS o CIFS.

NOTA: Esta función sólo funciona con direcciones IPv4. Por el momento, no se admiten direcciones IPv6.

La ruta de acceso a la imagen compartida CIFS debe tener el siguiente formato:

```
//<dirección IP o nombre de dominio>/<nombre_del_recurso_compartido>/<ruta_de_acceso_a_la_imagen>
```

La ruta de acceso a la imagen compartida NFS debe tener el siguiente formato:

```
<dirección_IP>:/<ruta_de_acceso_a_la_imagen>
```

Si el nombre de usuario incluye un nombre de dominio, el nombre de usuario deberá ser ingresado de la siguiente manera <nombre de usuario>@<dominio>. Por ejemplo, **usuario1@dell.com** es un nombre de usuario válido, mientras que **dell\usuario1** no lo es.

El nombre de archivo que termine con la extensión IMG es redireccionado como disco flexible virtual y el nombre de archivo que termine con la extensión ISO es redireccionado como CDROM virtual. El uso compartido de archivos remotos admite sólo formatos de archivo de imagen .IMG e .ISO.

La función RFS usa la implementación de medios virtuales subyacentes en iDRAC6. Debe tener privilegios de medios virtuales para realizar un montaje de RFS. Si medios virtuales ya utiliza una unidad virtual, la unidad no estará disponible para montar un RFS y viceversa. Para que RFS funcione, los medios virtuales en iDRAC6 deberán estar configurados en modos *Conectar* o *Conectar automáticamente*.

El estado de conexión para RFS se encuentra disponible en el registro de iDRAC6. Una vez conectado, un RFS montado en la unidad virtual no se desconecta, incluso si sale del iDRAC6. La conexión de RFS permanece cerrada si se restablece el iDRAC6 o pierde la conexión a la red. Las opciones interfaz gráfica del usuario y línea de comandos también se encuentran disponibles en CMC e iDRAC6 para cerrar la conexión del RFS. La conexión del RFS desde el CMC siempre anula el montaje de RFS existente en iDRAC6.

NOTA: La función VFlash del iDRAC6 y el RFS no están relacionados.

Para activar la función de archivos remotos compartidos a través de la interfaz web de iDRAC6, haga lo siguiente:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Seleccione **Sistema**→ ficha **Uso compartido de archivos remotos**.

   Aparece la pantalla **Uso compartido de archivos remotos**.

La Tabla 2-3 indica la configuración del uso compartido de archivos remotos.

Tabla 2-3. Configuración del servidor de archivos remotos

Atributo	Descripción
Nombre de usuario	Nombre de usuario para conectarse al sistema de archivos NFS/CIFS.
Contraseña	Contraseña para conectarse al sistema de archivos NFS/CIFS.

Ruta de acceso del archivo de imagen	Ruta de acceso del archivo que se compartirá a través del uso compartido de archivos remotos.
Estado	**Conectado**: El archivo se comparte. **No conectado**: El archivo no se comparte. **Conectando...:** Ocupado mientras se conecta al recurso compartido.

Haga clic en **Conectar** para establecer una conexión de uso compartido de archivos. El botón **Conectar** se desactiva una vez establecida la conexión.

NOTA: Incluso si ha configurado la función de archivos remotos compartidos, la interfaz gráfica de usuario no muestra esta información por razones de seguridad.

Para el uso compartido de archivos remotos, el comando de RACADM remoto es

`racadm remoteimage`.

`racadm remoteimage <opciones>`

Las opciones son:

`-c`; conectar imagen

`-d`; desconectar imagen

`-u <nombre_de_usuario>`; nombre de usuario para acceder al recurso compartido de red

`-p <contraseña>`; contraseña para acceder al recurso compartido de red

`-l <ubicación_de_imagen>`; ubicación de la imagen en el recurso compartido de red; indique la ubicación entre comillas dobles

`-s`; mostrar el estado actual

PRECAUCIÓN: Todos los caracteres, incluidos los especiales y alfanuméricos, están permitidos para nombre_de_usuario, contraseña y ubicación_de_imagen excepto los siguientes caracteres: ' (apóstrofo), " (comillas), , (comas), < (signo de menor) y > (signo de mayor). Al recurrir al uso compartido de archivos remotos, los caracteres anteriormente indicados no se permiten para el nombre de usuario, la contraseña y la ubicación de la imagen.

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 alguno de los métodos siguientes:

- Interfaz Web del iDRAC6
- CLI de RACADM
- 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 en **support.dell.com**. La imagen del firmware está disponible en varios formatos a fin de admitir los distintos métodos de actualización disponibles.

Para actualizar el firmware del iDRAC6 por medio de la interfaz web del iDRAC6 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 comprimidas 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 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 del 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: Si no se conserva la configuración durante la actualización del firmware, el iDRAC6 genera nuevas claves SHA1 y MD5 para el certificado SSL. Como las claves son diferentes a las del 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 el mensaje de error **Certificado no válido.**

NOTA: Si está realizando una reversión del firmware del iDRAC6 a una versión anterior, elimine el complemento ActiveX® existente del explorador Internet Explorer de cualquier estación de administración basada en Windows para permitir que el firmware instale una versión compatible del complemento ActiveX.

Verificación de la firma digital para los DUP de Linux

La firma digital se usa para autentificar la identidad del firmante de un archivo y para certificar que el contenido original del archivo no fue 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 estándar de verificación, realice los siguientes pasos:

1. Descargue la clave GnuPG pública de Linux de Dell de la siguiente manera: visite **lists.us.dell.com** y haga clic en el vínculo **Clave GPG pública de Dell**. Guarde el archivo en el sistema local. El nombre predeterminado es **linux-security- publickey.txt**.

2. Para importar la clave pública a la base de datos de confianza de GPG, ejecute el siguiente comando:

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

   NOTA: Debe tener la clave privada a la mano para completar el proceso.

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 siguiente mensaje:

      ```
      pub 1024D/23B66A9D 2001-04-16 Dell, Inc. (Product Group (Grupo de productos)) <linux-security@dell.com>
      Primary key fingerprint (Huella digital de clave primaria): 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.) (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 = I don't know or won't say (no sé o me abstengo)
        2 = I do NOT trust (no confío en él)
        3 = I trust marginally (confío en él con reservas)
        4 = I trust fully (confío en él)
        5 = I trust ultimately (confío en él plenamente)
        m = back to the main menu (regresar al menú principal)

      Your decision? (¿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? [s/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 DUP con la extensión **.sign**. Por ejemplo, la imagen del firmware del iDRAC6 tiene un archivo **.sign** asociado (**IDRAC_FRMW_LX_2.2.BIN.sign**) que se incluye en el archivo de extracción automática con la imagen del firmware (**IDRAC_FRMW_LX_2.2.BIN**). Para descargar los archivos, haga clic con el botón derecho del mouse en el vínculo de **descarga** y utilice la opción **"Guardar destino como..."**.

5. Verifique el paquete de actualización:

   `gpg --verify` *<nombre del 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 de Dell PowerEdge™ M610 del iDRAC6:

1. Descargue los dos archivos siguientes en **support.dell.com**:
   - IDRAC_FRMW_LX_2.2.BIN.sign
   - IDRAC_FRMW_LX_2.2.BIN

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

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

   Aparecerá el siguiente mensaje de salida:

   ```
   gpg: la clave 23B66A9D: "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>" not changed (no se modificó)
   gpg: Total number processed (Número total procesado): 1
   gpg: unchanged (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 el símbolo del sistema, 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 Dell PowerEdge M610 del iDRAC6 mediante la ejecución del comando siguiente:

   ```
   gpg --verify IDRAC_FRMW_LX_2.2.BIN.sign IDRAC_FRMW_LX_2.2.BIN
   ```

   Aparecerá el siguiente mensaje de salida:

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

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

```
gpg: WARNING: This key is not certified with a trusted signature! (ADVERTENCIA: Esta clave no está certificada con una firma confiable.)
gpg: There is no indication that the signature belongs to the owner. (No hay indicación de que la firma pertenezca al propietario.)
Primary key fingerprint (Huella digital de clave primaria): 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
```

Uso de la interfaz web del iDRAC6

NOTA: Si se interrumpe el progreso de la actualización del firmware del iDRAC6 antes de que se complete, el firmware del iDRAC6 se dañará. En tal caso, puede recuperar el iDRAC6 desde la interfaz web del CMC.

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\V2.1\<nombre_de_imagen>`.

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

5. Haga clic en **Cargar**.

   El archivo se cargará en el iDRAC6. Este proceso podría tardar varios minutos.

   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 termina de cargarse y pasa todas las revisiones de verificación, aparece 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 de marcación **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 o a través del CMC.

6. De manera predeterminada, la casilla de marcación **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 de marcación **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, aparece 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 desde una ventana nueva de explorador.

Actualización del firmware del iDRAC6 por medio de RACADM

Puede actualizar el firmware del iDRAC6 mediante RACADM remoto.

1. Puede descargar la imagen del firmware del iDRAC6 en el sistema administrado a través del sitio web de asistencia de Dell en **support.dell.com**.

   Por ejemplo:

   `C:\downloads\firmimg.imc`

2. Ejecute el siguiente comando de RACADM:

   Por ejemplo:

   `racadm -r <dirección IP del iDRAC6> -u <nombre de usuario> -p <contraseña> fwupdate -g -u -a <ruta de acceso>`

   donde *ruta de acceso* es la ubicación en el servidor TFTP en la que está almacenado **firmimg.imc**.

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 la opción adicional -nopresconfig en el mensaje de salida sobre el uso. Esta opción se usa para actualizar el firmware sin conservar la información de configuración. Se recomienda **no** usar esta opción ya que *elimina* toda su información de configuración del iDRAC6, como direcciones IP, usuarios y contraseñas.

Limpiar el caché del explorador

Para usar las funciones más recientes del iDRAC6, borre el caché del explorador para eliminar las páginas web *antiguas* que puedan estar almacenadas en el sistema.

Actualización del paquete de reparación de USC

Consulte la *Guía del usuario de Dell Lifecycle Controller* 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 versión 2.0 de la interfaz de administración de plataforma inteligente (IPMI).

El iDRAC6 cumple con IPMI versión 2.0. En esta sección se describen los pasos necesarios para configurar el 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 (tarjeta) 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 iDRAC6, utilice las teclas de flechas para desplazarse hacia abajo.

1. Activar **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 implementarse 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.

NOTA: También puede usar Dell Management Console, la aplicación de administración de uno a varios sistemas de próxima generación, para activar el descubrimiento y la supervisión. Para obtener más información, consulte la *Guía del usuario de Dell Management Console* en el sitio web de asistencia de Dell' en **support.dell.com / manuals**.

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 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 **Red**.

5. Haga clic en **Configuración de IPMI**.

6. Asegúrese de que la casilla de marcación **Activar IPMI en la LAN** esté seleccionada.

7. Seleccione **Administrador** en el menú desplegable **Límite de nivel de privilegio del 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 las alertas por correo electrónico para uno o más sucesos seleccionando la casilla en la columna **Generar alertas.**

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

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

    Aparecerá la pantalla **Configuración de captura**.

15. En el primer campo disponible **Dirección IP de destino** de la sección **Lista de destinos de iPv4**, seleccione la casilla de marcación **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 aparte 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 **Red/Seguridad** y luego 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 de marcación **Activar usuario**, y luego escriba el nombre de usuario y la contraseña.

5. En la sección **Privilegios de LAN de IPMI**, 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 el descubrimiento, los dispositivos 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 DRAC 5, en los que la tarjeta de administración aparece en el grupo de RAC.

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*.

NOTA: También puede usar Dell Management Console, la aplicación de administración de uno a varios sistemas de próxima generación, para ver los sucesos y el estado del iDRAC6. Para obtener más información, consulte la *Guía del usuario de Dell Management Console* en el sitio web de asistencia de Dell en **support.dell.com / manuals**.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la estación de administración

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Una estación de administración es un equipo que se usa para supervisar y administrar los servidores Dell 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 web admitido.
3. Instale Java® Runtime Environment (JRE) (necesario si usa Firefox).
4. Instale clientes SSH o Telnet, de ser necesario.
5. Instale a un servidor TFTP, de ser necesario.
6. Instale Dell OpenManage IT Assistant (opcional).
7. Instale Dell Management Console (DMC) (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 diversas funciones de administración en el servidor administrado, como por ejemplo reiniciar el equipo y usar los servicios del iDRAC6. Sin embargo, para tener acceso a la red y a los servicios de aplicación que se encuentran en el servidor administrado, es posible que necesite tener una NIC adicional en el servidor administrado.

Configuración de un explorador web admitido

Las secciones siguientes contienen instrucciones para configurar los exploradores web admitidos para usar con la interfaz web del iDRAC6.

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 visualizar la interfaz y acceder a todas las funciones, asegúrese de que su resolución esté configurada al menos en 800 por 600 píxeles y/o cambie el tamaño del 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 procesada 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 que se conecta 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 secuencias de comandos: Habilitar
   - Descargar los controles ActiveX firmados: Preguntar
   - Inicializar y generar secuencias de comandos de los controles ActiveX no marcados como seguros: Preguntar
   - Ejecutar controles y complementos de ActiveX: Habilitar
   - Generar secuencias de comandos de los controles ActiveX marcados como seguros para Secuencias de comandos: 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 secuencias de comandos en el control del explorador web de Internet Explorer: Habilitar
   - Permitir que se abran ventanas generadas por secuencias de comandos sin restricción de tamaño ni 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**:

   - Secuencia de comandos activa: Habilitar
   - Permitir operaciones de pegado por medio de una secuencia de comandos: Habilitar
   - Secuencias de comandos de applets de Java®: Habilitar

- Seleccione **Herramientas**→ **Opciones de Internet**→ **Opciones avanzadas**.
- 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 secuencias de comandos (Internet Explorer): Seleccionada
  - Deshabilitar la depuración de secuencias de comandos (otros): Seleccionada
  - Mostrar una notificación sobre cada error de secuencia de comandos: 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, se recomienda aprender y comprender correctamente las consecuencias de cada 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 del iDRAC6 a través del explorador web, es posible que se le pida que agregue la dirección IP del 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 del iDRAC6.

Es posible que en algunos sistemas operativos Internet Explorer (IE) 8 no le solicite que agregue la dirección IP de iDRAC6 a la lista de los dominios de confianza si la dirección no está incluida en la lista.

Para agregar la dirección IP de iDRAC6 a la lista de los dominios de confianza en IE8, haga lo siguiente:

1. Seleccione **Herramientas→ Opciones de Internet→ Seguridad→ Sitios de confianza→ Sitios**.
2. Introduzca la dirección IP de iDRAC6 en **Agregar este sitio web a la zona**.
3. Haga clic en **Agregar**.
4. Haga clic en **Aceptar**.
5. Haga clic en **Cerrar**.
6. Haga clic en **Aceptar** y actualice el explorador.

Al iniciar el vKVM por primera vez a través de IE8 con el complemento Active-X, puede aparecer el mensaje "`Error de certificado: Navegación bloqueada`".

1. Haga clic en **Continuar a este sitio web**.

2. Haga clic en **Instalar** para instalar los controles Active-X en la ventana **Advertencia de seguridad**.

La sesión de vKVM se iniciará.

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 admitidos. El uso de la interfaz con otros dialectos o idiomas no es compatible y puede no funcionar como se desea. Para algunos idiomas admitidos, es posible que se deba ajustar el tamaño de la ventana del explorador a 1024 píxeles 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 acceder a algunas funciones o letras. Para obtener más detalles sobre cómo usar su teclado localizado en estos casos, consulte "Uso de Video Viewer". No se admiten otros teclados y su uso puede causar problemas inesperados.

NOTA: Consulte la documentación del explorador que indica cómo configurar diferentes idiomas y visualizar versiones localizadas de la interfaz web del iDRAC6.

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 para el 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:

   Entrada actual:

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

   Entrada 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 iníciela en el sistema operativo.

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

Desactivación de la función de lista blanca en Firefox

Firefox tiene una función de seguridad denominada "lista blanca" que requiere permiso del usuario para instalar complementos para cada sitio distinto que aloje un complemento. Cuando está activada, la función de lista blanca requiere que se instale un visor de redirección de consola por cada iDRAC6 que se 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 de que **Valor** sea **true**. Si no lo es, haga doble clic en **xpinstall.enabled** para cambiar el **Valor** a **true**.

Instalación del software del iDRAC6 en la estación de administración

El sistema incluye el DVD *Dell Systems Management Tools and Documentation*. Este DVD ofrece los siguientes componentes:

- Directorio raíz del DVD: Contiene Dell Systems Build and Update Utility, que proporciona información sobre la instalación y configuración del servidor y del sistema.
- SYSMGMT: Contiene productos de software de administración de sistemas, incluido Dell OpenManage Server Administrator

Instalación y desinstalación de RACADM en una estación de administración

Para usar las funciones remotas de RACADM, instale RACADM en una estación de administración. Consulte la *Guía de instalación de Dell OpenManage Management Station Software* disponible en **support.dell.com/manuals** para obtener información sobre cómo instalar las herramientas de DRAC en una estación de administración cuyo sistema operativo es Microsoft Windows.

Instalación y desinstalación de RACADM en Linux

1. Inicie sesión como usuario "root" en el sistema en donde desea instalar los componentes de la estación de administración.
2. De ser necesario, monte el DVD *Dell Systems Management Tools and Documentation* con el comando siguiente o un comando similar:

   ```
   mount /media/cdrom
   ```
3. Diríjase al directorio **/linux/rac** y ejecute el comando siguiente:

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

Para recibir ayuda con el comando RACADM, escriba **racadm help** después de enviar los comandos anteriores.

Para desinstalar RACADM, abra un símbolo de comando y escriba:

```
rpm -e <nombre_del_paquete_de_racadm>
```

donde *<nombre_del_paquete_de_racadm>* es el paquete RPM que se usó para instalar el software del iDRAC6.

Por ejemplo, si el nombre del paquete RPM es **srvadmin-racadm5**, escriba:

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

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 Firefox si instala JRE y configura el visor de consola en la interfaz web del iDRAC6 antes de iniciar el visor. Consulte "Configuración de la redirección de consola y los 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: El iDRAC6 admite un máximo de 4 sesiones de Telnet y 4 sesiones de SSH de forma simultánea.

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 que la versión estándar que se incluye en el sistema operativo.

Si la estación de administración ejecuta Windows XP SP1 o Windows 2003, es posible que tenga un problema con los caracteres en una sesión Telnet del 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 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 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 siguiente mensaje:

   ```
   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.

Puede usar programas como PuTTY u OpenSSH 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 **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 el símbolo del sistema de Windows no produce una funcionalidad completa (es decir, algunas teclas no responden y no se muestran gráficos).

El iDRAC6 admite un máximo de 4 sesiones de Telnet y 4 sesiones de SSH de forma simultánea. Sin embargo, sólo una de las 8 posibles sesiones puede usar SM-CLP. Es decir, el iDRAC6 admite solamente una sesión SM-CLP por vez. 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 Enterprise".

La implementación de SSH del iDRAC6 admite varios esquemas de criptografía, según se muestra en 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 un 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 RACADM cuando realice estas tareas, deberá tener un servidor TFTP funcionando en un equipo al que el iDRAC6 pueda tener acceso por medio de la dirección 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 de Dell y archivos léame: consulte los archivos léame y el sitio web de asistencia de Dell en **support.dell.com/manuals** para consultar la información más reciente sobre los productos Dell.

Para obtener información sobre la instalación de IT Assistant, consulte la *Guía del usuario de Dell OpenManage IT Assistant* que se encuentra disponible en **support.dell.com/manuals**.

Instalación de Dell Management Console

Dell Management Console (DMC) es la aplicación de próxima generación para la administración de uno a varios sistemas que ofrece una funcionalidad similar a la de Dell OpenManage IT Assistant y también incluye funciones mejoradas de descubrimiento, inventario, supervisión e informes. Se trata de una interfaz gráfica para el usuario basada en web que se instala en una estación de administración en un entorno de red.

Puede instalar DMC desde el DVD *Dell Management Console* o descargarlo e instalarlo desde el sitio web de Dell en **www.dell.com/openmanage**.

Consulte la *Guía del usuario de Dell Management Console User* disponible en **support.dell.com/manuals** para consultar las instrucciones de instalación del software.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración del servidor administrado

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

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:

- Interfaz de línea de comandos de RACADM: Permite administrar y configurar el iDRAC6. Es una herramienta potente para efectuar tareas de configuración y administración de secuencias de comando.
- Server Administrator: Se requiere que 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* para instalar Dell OpenManage Server Administrator. Para obtener las instrucciones para instalar este software, consulte la *Guía de instalación de Dell OpenManage Server Administrator* que se encuentra disponible en **support.dell.com/manuals**.

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 y tratar de 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, consulte la *Guía de instalación de Dell OpenManage Server Administrator* y la *Guía de instalación de Dell OpenManage Management Station Software*. Puede acceder a estos documentos en el sitio web de asistencia de Dell en **support.dell.com/manuals**.

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

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

   Para activar la pantalla del último bloqueo por medio de RACADM local, abra una petición de comandos en el servidor administrado y escriba el comando siguiente:

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

4. En la interfaz web de Server Administrator, active el temporizador de **Recuperación automática** y 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 Dell OpenManage 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 de 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

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

El iDRAC6 ofrece una interfaz web que permite configurar las propiedades y los usuarios del iDRAC6, realizar tareas de administración remota y solucionar problemas de un sistema (administrado) remoto. Por lo general, usará la interfaz web para realizar las tareas diarias de administración de sistemas. Este capítulo proporciona información sobre cómo realizar tareas comunes de administración de sistemas con la interfaz web del iDRAC6 y proporciona vínculos a información relacionada.

La mayoría de las tareas de configuración para las que usará la interfaz web también se pueden realizar con comandos de RACADM local o remoto o bien con comandos de SM-CLP.

Los comandos de RACADM local se ejecutan desde el servidor administrado. RACADM remoto es una utilidad cliente que se ejecuta en una estación de administración y usa la interfaz fuera de banda para comunicarse con el servidor administrado. Esta utilidad se usa con la opción **-r** para ejecutar los comandos a través de una red. Para obtener más información sobre RACADM, consulte "Uso de la interfaz de línea de comandos de RACADM".

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

Acceso a la interfaz web

Para acceder a la interfaz web del iDRAC6, realice los pasos que se indican a continuación:

1. Abra una ventana de un explorador web compatible.
2. En el campo **Dirección**, escriba `https://<Dirección_IP_del_iDRAC6>` y presione <Entrar>.

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

   `https://<dirección_IP_del_iDRAC6>:<número_de_puerto>`

   donde *dirección_IP_del_iDRAC6* es la dirección IP del iDRAC6 y *número_de_puerto* es el número del puerto HTTPS.

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

Inicio de sesión

Puede iniciar sesión como usuario del iDRAC6, como usuario de Microsoft® Active Directory®, o como usuario del LDAP. 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 iniciar sesión, realice los pasos siguientes:

1. En el campo **Nombre de usuario**, escriba uno de los siguientes valores:
   - Su nombre de usuario del iDRAC6.

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

   - Su nombre de usuario de Active Directory (AD). También puede seleccionar el nombre del dominio AD del menú desplegable.

     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**.

   - Nombre de usuario de LDAP (sin nombre de dominio).
- En el campo **Contraseña**, introduzca su contraseña de usuario del iDRAC6, su contraseña de usuario de Active Directory o su contraseña del LDAP. Las contraseñas distinguen entre mayúsculas y minúsculas.
- Haga clic en **Aceptar** o presione <Entrar>.

Cierre de sesión

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

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

NOTA: Cerrar el explorador sin desconectarse como corresponde puede hacer que la sesión permanezca activa hasta que expire el tiempo de la misma. Se recomienda que haga clic en el botón **Cerrar sesión** para finalizar una sesión.

NOTA: Si se cierra la interfaz web del 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**.

PRECAUCIÓN: Si ha abierto múltiples sesiones de la interfaz web de usuario mediante <Ctrl+T> o <Ctrl+N> para acceder al mismo iDRAC6 desde una misma estación de administración y luego cierra alguna de las sesiones, todas finalizarán.

Uso de varias fichas y ventanas del explorador

Las distintas versiones de exploradores Web muestran diferentes comportamientos al abrir nuevas fichas y ventanas. 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 (IE) 7 e IE 8 ofrecen la opción de abrir fichas además de ventanas. Cada ficha hereda las características de la ficha abierta más recientemente. Presione <Ctrl–T> para abrir una nueva ficha y <Ctrl–N> para abrir una nueva ventana del explorador desde la sesión activa. Iniciará sesión con las credenciales ya autentificadas. Al cerrar una ficha finalizan todas las fichas de interfaz Web de iDRAC6. Asimismo, 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.

La acción de las fichas en Firefox 2 y Firefox 3 es igual que en IE 7 e IE 8: Nuevas fichas inician nuevas sesiones. Sin embargo, el comportamiento 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 IE 7 e IE 8	Desde la última sesión abierta	Nueva sesión
Firefox 2 y Firefox 3	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 está accesible' en la red. Consulte "Configurar el sistema de red del iDRAC6" para obtener ayuda con la configuración inicial de la red del iDRAC6.

Configuración de los valores de VLAN, de IPMI y de red

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

NOTA: La mayoría de los servidores DHCP requiere un servidor para guardar un testigo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC6) debe proporcionar este testigo 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**→ **iDRAC6**.
2. Haga clic en la ficha **Red/Seguridad**.

   Aparece la pantalla **Red**.
3. Configure la red, IPMI y VLAN según sea necesario. Consulte la Tabla 5-2, la Tabla 5-3 y la Tabla 5-4 para ver descripciones de las opciones de configuración de **red, IPMI** y **VLAN**.
4. Haga clic en **Aplicar**.
5. Para continuar, haga clic en el botón correspondiente.

Tabla 5-2. Configuración de red

Valor	Descripción
Configuración de tarjeta de interfaz de red	
Dirección MAC	Muestra la dirección de control de acceso al medio (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red. La dirección MAC no se puede cambiar.
Activar el NIC	Cuando se selecciona, indica que el NIC está activado y habilita los controles restantes en este grupo. Cuando el NIC está desactivado, se bloquea toda la comunicación con el iDRAC6 a través de la red. El valor predeterminado es **Deseleccionado**.
Valores comunes	
Registrar iDRAC6 en el DNS	Registra el nombre del iDRAC6 en el servidor DNS. El valor predeterminado es **Deseleccionado**.
iDRAC6 en DNS Nombre	Muestra el nombre del iDRAC6. 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-HM8912S.
Usar DHCP para el nombre del dominio de DNS	**Seleccionado**: Activar adquisición de DNS mediante DHCP. **Deseleccionado**: Desactivar adquisición de DNS mediante DHCP.
Nombre de dominio de DNS	El **nombre de dominio de DNS** predeterminado está en blanco. Cuando la casilla **Usar DHCP para el nombre de dominio de DNS** está seleccionada, esta opción aparece en gris y el campo no se puede modificar.
Configuración de IPv4	
Activado	Activa (**Seleccionado**) o desactiva (**Deseleccionado**) la compatibilidad con el protocolo IPv4. La opción **Activar el NIC** debe estar seleccionada para activar este valor.
Activar DHCP	Si está **seleccionado**, Server Administrator obtiene la dirección IP para el NIC del iDRAC6 desde el servidor DHCP. También desactiva los campos **Dirección IP**, **Máscara de subred** y **Puerta de enlace**.
Dirección IP	Permite introducir o editar una dirección IP estática para el NIC del iDRAC6. Para cambiar este valor, deseleccione la opción **Activar DHCP**.
Máscara de subred	Permite introducir o editar una máscara de subred para el NIC del iDRAC6. Para cambiar este valor, deseleccione la opción **Activar DHCP**.
Puerta de enlace	Permite introducir o editar una puerta de enlace estática IPv4 para el NIC del iDRAC6. Para cambiar este valor, deseleccione la opción **Activar DHCP**.
Usar DHCP para obtener direcciones del servidor DNS	Seleccione la opción **Activar DHCP** para obtener direcciones de servidores DNS al seleccionar la casilla **Usar DHCP para obtener direcciones del servidor DNS**. Cuando no se use el DHCP para obtener las direcciones de servidores DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.
Servidor DNS preferido	Permite introducir o editar una dirección IP estática para el servidor DNS preferido. Para cambiar este valor, deseleccione primero la opción **Usar DHCP para obtener direcciones del servidor DNS**.
Servidor DNS alternativo	Utiliza la dirección IP del servidor DNS secundario cuando la opción **Usar DHCP para obtener direcciones del servidor DNS no está seleccionada**. Introduzca una dirección IP 0.0.0.0 si no hay ningún servidor DNS alternativo.
Configuración de IPv6	
Activado	Si la casilla está **seleccionada**, IPv6 está activado. Si la casilla **no está seleccionada**, IPv6 está desactivado. El valor predeterminado es **Deseleccionado**.
Activar configuración automática	Seleccionar esta opción le permite al iDRAC6 obtener la dirección IPv6 para el NIC del iDRAC6 desde el servidor del Protocolo de configuración dinámica de host (DHCPv6). Al habilitar **Activar configuración automática** también se desactivan y vacían los valores estáticos para **Dirección IPv6**, **Longitud de prefijo** y **Puerta de enlace**.
Dirección IPv6	Configura la dirección IPv6 para el NIC del iDRAC6. Para cambiar estos valores, primero debe deshabilitar la opción **Activar configuración automática** deseleccionando la casilla relacionada. **NOTA:** Sólo dos direcciones IPv6 (la dirección local del vínculo y la dirección global) se muestran si la configuración de la red tiene definido DHCP IPv6 y las dieciséis direcciones IPv6 se mostrarán si configuró el enrutador de red para enviar mensajes de anuncios del enrutador. **NOTA:** iDRAC6 no permite guardar la configuración si introduce una dirección IPv6 que conste de más de ocho grupos.
Longitud del prefijo	Configura la longitud de prefijo de la dirección IPv6. Se puede valuar entre 1 y 128 inclusive. Para cambiar estos valores, primero debe deshabilitar la opción **Activar configuración automática** deseleccionando la casilla relacionada.
Puerta de enlace	Configura la puerta de enlace IPv6 estática para el NIC del iDRAC6. Para cambiar estos valores, primero debe deshabilitar la opción **Activar configuración automática** deseleccionando la casilla relacionada.
Use el DHCPv6 para obtener direcciones de servidor DNS	Active el DHCP para obtener direcciones del servidor DNS IPv6 seleccionando la casilla **Usar DHCPv6 para obtener direcciones del servidor DNS**. Cuando no se usa DHCP para obtener las direcciones de servidores DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**. El valor predeterminado es **deseleccionado**. **NOTA:** Cuando la casilla **Usar DHCPv6 para obtener direcciones del servidor DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.
Servidor DNS preferido	Especifica la dirección IPv6 estática del servidor DNS preferido. Para cambiar este valor, deseleccione **Usar DHCPv6 para obtener direcciones de servidor DNS**.
Servidor DNS alternativo	Especifica la dirección IPv6 estática del servidor DNS alternativo. Para cambiar este valor, deseleccione **Usar DHCPv6 para obtener direcciones de servidor DNS**.

Tabla 5-3. Configuración de IPMI

Valor	Descripción
Activar IPMI en la LAN	Cuando está seleccionado, indica que el canal LAN de IPMI está activado. El valor predeterminado es **Deseleccionado**.
Límite del nivel de privilegios del canal	Configura el nivel máximo de privilegios 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. La clave de cifrado debe consistir en un número par de caracteres hexadecimales con un máximo de 40 caracteres sin espacios. La clave predeterminada de IPMI sólo contiene ceros.

Tabla 5-4. Configuración de VLAN

Botón	Descripción
Activar identificación de VLAN	**Sí**: Activada. **No**: Desactivada. Si esta opción está activada, sólo se aceptará el tráfico con identificación de LAN virtual (VLAN) que coincida. **NOTA:** La configuración de VLAN sólo puede definirse a través de la interfaz web de CMC. El iDRAC6 sólo muestra el estado actual de activación; no puede modificar los valores en esta pantalla.
Identificación de VLAN	Campo Identificación de VLAN de campos de 802.1g. Muestra un valor de 1 a 4094, excepto de 4001 a 4020.
Prioridad	Campo Prioridad de campos de 802.1g. Este campo se utiliza para determinar la prioridad de la identificación de VLAN y muestra un valor de 0 a 7 para el nivel de prioridad de VLAN.

Tabla 5-5. Botones de configuración de la red

Botón	Descripción
Configuración avanzada	Muestra la pantalla **Seguridad de la red**, lo que permite al usuario introducir 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 **Red**.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la pantalla de configuración de la red. **NOTA:** Los cambios en la configuración de la dirección IP del NIC cierran todas las sesiones de usuario, por lo tanto, los usuarios deben volver a conectarse a la interfaz web del iDRAC6 con la configuración actualizada de la dirección IP. Todos los demás cambios requieren que se restablezca la tarjeta de interfaz de red, lo que provocará una breve pérdida de conectividad.

Configuración del filtrado de IP y bloqueo de IP

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

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

   Aparece la pantalla **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 Tabla 5-6 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. Consulte Tabla 5-7.

Tabla 5-6. Configuración de filtrado y bloqueo de IP

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 **Desactivado**.
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 **Desactivado**.
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 5-7. 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 configuración de la 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 5-8.

Tabla 5-8. Sucesos de plataforma que se pueden filtrar

Índice	Suceso de plataforma
1	Advertencia de sonda de baterías
2	Falla de sonda de baterías
3	Falla de sonda de voltaje discreto
4	Advertencia de sonda de temperatura
5	Falla de sonda de temperatura
6	Falla del procesador
7	Procesador ausente
8	Falla del registro de hardware
9	Recuperación automática del sistema
10	Falla de la tarjeta SD
11	Redundancia perdida

Cuando se presenta un suceso de plataforma (por ejemplo, una *advertencia de sonda de la batería*), se genera un suceso del sistema que 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 PET 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 filtros de sucesos de plataforma (PEF)

NOTA: Configure los filtros de sucesos de plataforma antes de configurar la captura 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 opción **Generar alerta** al lado de cada suceso para que desee generar 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: La casilla de sucesos **Generar alerta** debe estar seleccionada para que se pueda enviar un alerta para ese suceso.

Configuración de capturas de sucesos de plataforma (PET)

NOTA: Debe tener permiso para **Configurar el iDRAC** para agregar, activar o desactivar una alerta SNMP. Las opciones siguientes no estarán disponibles si no se 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 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 **Valores de captura**.

   Aparecerá la pantalla **Valores de captura.**

5. Configure la dirección IP de destino de la PET:

   a. Seleccione la casilla **Activado** junto al **Número de destino** que desea activar.

   b. Introduzca una dirección IP en el cuadro correspondiente **Dirección IP de destino** IPv4 o IPv6.

   NOTA: La cadena de comunidad de destino debe ser la misma que la cadena de comunidad del iDRAC6.

   c. Haga clic en **Aplicar**.

   NOTA: Para enviar una captura correctamente, configure el valor de **Cadena de comunidad**. El valor de **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 IP de destino adicional, repita del paso a al paso d. Puede especificar hasta cuatro direcciones de destino IPv4 y cuatro IPv6.

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 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, el servidor SMTP (correo electrónico) debe estar configurado en la sección **Configuración de dirección del servidor SMTP (correo electrónico)** de la pantalla **Configuración de alertas de correo electrónico**. Especifique un servidor SMTP en el campo provisto usando el formato de números separados por puntos (por ejemplo: 192.168.1.1) o el nombre DNS. La dirección IP del Servidor SMTP se comunica con el iDRAC6 para enviar alertas por correo electrónico cuando ocurre un suceso de plataforma.

   d. En el campo **Modificar nombre de correo electrónico de origen**, introduzca el correo electrónico iniciador del alerta, o bien deje el campo en

blanco para usar el correo electrónico iniciador predeterminado. El correo predeterminado es blade_slot@iDRAC6 Dirección IP.

- Si el campo **Modificar nombre de correo electrónico de origen** está en blanco, el nombre de host del iDRAC6 está configurado y el nombre del dominio DNS está activo, entonces la dirección de correo electrónico de origen es: <nombre de host iDRAC6>@<Nombre del dominio DNS>.
- Si el campo está en blanco, el nombre de host del iDRAC6 está en blanco, y el nombre del dominio DNS está activo, entonces la dirección de correo electrónico de origen es: <iDRAC6 Slot*x*>@<Nombre del dominio DNS>.
- Si el campo está en blanco, el nombre de host del iDRAC6 está en blanco y el nombre del dominio DNS está en blanco, entonces la dirección de correo electrónico de origen es: <iDRAC6 Slotx>@<Dirección IP de iDRAC6>.
- Si el campo es "una cadena sin @", y el nombre del dominio DNS está activa, entonces la dirección de correo electrónico de origen es: <cadena sin @>@<Nombre del dominio DNS>.
- Si el campo es "una cadena sin @", y el nombre del dominio DNS está en blanco, entonces la dirección de correo electrónico de origen es: <cadena sin @>@<Dirección IP de iDRAC6>.
- Si el campo es "una cadena sin @", y el nombre del dominio DNS está activa, entonces la dirección de correo electrónico es: <cadena sin @>@<Nombre del dominio DNS>.
- Si el campo es "una cadena con @", y el nombre del dominio DNS está en blanco, entonces la dirección de correo electrónico de origen es: <cadena con @>@<Dirección IP de iDRAC6>.

e. Haga clic en **Enviar** para probar la alerta por correo electrónico configurada (si lo desea).

f. Para agregar un destino de alertas por correo electrónico adicional, repita del paso a al paso e. 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**→ **iDRAC6**, luego haga clic en la ficha **Red/Seguridad**.

   Aparecerá la pantalla **Red**.

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

   c. Seleccione la casilla **Activar IPMI en la LAN**.

   d. Actualice el **Límite de nivel de privilegio del canal**, 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 de IPMI 2.0.

   En **Configuración de 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 del iDRAC6 es compatible con el protocolo RMCP+.

   En **Configuración de 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**→ **iDRAC6**, luego haga clic en la ficha **Red/Seguridad**.

   Aparecerá la pantalla **Red**.

   b. Haga clic en la ficha **Comunicación en serie en la LAN**.

   c. Seleccione **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**.

   f. Configure los valores de filtrado y bloqueo de IP según sea necesario en la página **Configuración avanzada**.

Cómo agregar y configurar usuarios del 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 usuarios del iDRAC6, realice los pasos a continuación:

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

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC6**→ **Red / Seguridad**→ **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.

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

3. En la página **Menú principal del usuario** (consulte Tabla 5-9, Tabla 5-10 y Tabla 5-11), puede configurar un usuario, cargar un archivo de clave pública de SSH o ver o eliminar una clave específica o todas las claves de SSH.

Autentificación de la clave pública en el SSH

El iDRAC6 admite la autentificación de clave pública (PKA) a través de SSH. Este método de autentificación mejora la automatización de secuencias de comandos de SSH al eliminar la necesidad de incorporar o solicitar la identificación/contraseña del usuario.

Antes de comenzar

Puede configurar hasta 4 claves públicas *por usuario* que pueden ser utilizadas en la interfaz de SSH. Antes de agregar o eliminar claves públicas, no deje de usar el comando view para ver las claves que ya están configuradas y no sobrescribir ni eliminar accidentalmente una de ellas. Cuando la PKA en SSH está configurada y se utiliza correctamente, no es necesario que escriba la contraseña al iniciar sesión en el iDRAC6. Esto puede ser muy útil para configurar secuencias de comandos automatizadas para realizar distintas funciones.

Cuando se prepare para configurar esta funcionalidad, tenga en cuente lo siguiente:

- Puede administrar está función con RACADM y desde la GUI.
- Al agregar claves públicas nuevas, verifique que las claves existentes no se encuentren ya en el índice donde se agregará la clave nueva. iDRAC6 no realiza comprobaciones para verificar que las claves anteriores se han eliminado antes de agregar una nueva. Tan pronto se agrega una clave nueva, está automáticamente vigente siempre que la interfaz de SSH esté activada.

Generación de claves públicas para Windows

Antes de agregar una cuenta, se requiere una clave pública del sistema que accederá al iDRAC6 en el SSH. Hay dos maneras de generar el par de claves públicas/privadas: Usando la aplicación *Generador de claves PuTTY* para clientes que ejecutan Windows o la CLI *ssh-keygen* para clientes que ejecutan Linux. La utilidad de CLI *ssh-keygen* está incluida de forma predeterminada en todas las instalaciones estándar.

Esta sección describe instrucciones sencillas para generar un par de claves públicas/privadas para ambas aplicaciones. Para ver usos adicionales o avanzados de estas herramientas, consulte la ayuda de la aplicación.

Para usar el *generador de claves PuTTY* para los clientes de Windows y crear la clave básica:

1. Inicie la aplicación y seleccione SSH-2 RSA o SSH-2 DSA para el tipo de clave que generará. SSH-1 no es compatible.

2. Escriba el número de bits para la clave. Los algoritmos admitidos para generar claves son RSA y DSA únicamente. El número tiene que estar entre los 768 y los 4096 bits para RSA y 1024 bits para DSA.

3. Haga clic en **Generar** y mueva el mouse dentro de la ventana como se indica. Luego de crear la clave, se puede modificar el campo de comentario de clave. También se puede escribir una frase contraseña para asegurar la clave. Verifique que ha guardado la clave privada.

4. Puede guardar la clave pública en un archivo usando la opción **Guardar clave pública** para cargarla más tarde. Todas las claves cargadas deben estar en formato RFC 4716 u openSSH. De lo contrario, deberá convertirlas a estos formatos.

Generación de claves públicas para Linux

La aplicación *ssh-keygen* para clientes Linux es una herramienta de línea de comandos sin interfaz gráfica de usuario.

Abra una ventana de terminal y en el indicador de shell escriba:

```
ssh-keygen –t rsa –b 1024 –C testing
```

NOTA: Las opciones distinguen entre mayúsculas y minúsculas.

Donde:

-t puede ser *dsa* o *rsa*.

la opción **-b** especifica el tamaño de cifrado de bits entre 768 y 4096.

la opción **-C** permite modificar el comentario de clave pública y es opcional.

Después de que el comando se ejecute, cargue el archivo público.

NOTA: Las claves generadas desde la estación de administración con Linux usando ssh-keygen no se encuentran en formato RFC4716, pero sí en openSSH. Las claves públicas en formato openSSH pueden ser cargadas en iDRAC6. El algoritmo de clave pública iDRAC6 valida ambas claves, la openSSH y la RFC4716, internamente convierte las claves RFC4716 al formato openSSH, e internamente las almacena.

NOTA: iDRAC6 no admite el envío ssh-agent de claves.

Inicio de sesión con autentificación de clave pública

Una vez que las claves públicas han sido cargadas, puede iniciar sesión en iDRAC6 en el SSH sin tener que introducir una contraseña. También tendrá la opción de enviar un solo comando de RACADM como argumento de línea de comandos a la aplicación de SSH. Las opciones de línea de comandos se comportan como RACADM remoto ya que la sesión finaliza al completarse el comando.

Por ejemplo:

Inicio de sesión:

```
ssh username@<dominio>
```

O bien:

```
ssh username@<dirección_IP>
```

donde dirección_IP es la dirección IP del iDRAC6.

Envío de comandos RACADM:

```
ssh username@<dominio> racadm getversion
```

```
ssh username@<dominio> racadm getsel
```

Consulte "Carga, visualización y eliminación de claves SSH por medio de RACADM" para obtener información sobre cómo cargar, ver y eliminar claves SSH usando RACADM.

Tabla 5-9. Configuraciones de claves SSH

Opción	Descripción
Cargar clave(s) SSH	Permite al usuario local cargar un archivo de clave pública SSH. Si carga una clave, el contenido del archivo de la clave aparece en un cuadro de texto no editable, en la página **Configuración del usuario**.
Ver o quitar clave (s) SSH	Permite al usuario local ver o eliminar una clave SSH especificada o todas las claves SSH.

La página **Cargar clave(s) SSH** le permite cargar un archivo de clave pública SSH. Si carga una clave, el contenido del archivo de la clave aparece en un cuadro de texto no editable en la página **Ver o quitar clave(s) SSH**.

Tabla 5-10. Cargar clave(s) SSH

Opción	Descripción
Archivo o texto	Seleccione la opción **Archivo** y escriba la ruta de acceso donde se encuentra la clave. También puede seleccionar la opción **Texto** y copiar el contenido del archivo de la clave en el cuadro. Puede cargar nuevas claves o sobrescribir las existentes. Para cargar un archivo de clave, haga clic en **Explorar**, seleccione el archivo y haga clic en el botón **Aplicar**. **NOTA:** La opción pegar texto de clave es admitida para claves públicas en el formato openSSH. La opción para pegar texto no está admitida para el formato RFC4716.
Explorar	Haga clic en este botón para ubicar la ruta de acceso completa y el nombre del archivo de la clave.

La página **Ver o quitar clave(s) SSH** le permite ver o quitar las claves públicas SSH del usuario.

Tabla 5-11. Ver o quitar clave(s) SSH

Opción	Descripción
Quitar	En el cuadro aparece la clave cargada. Seleccione la opción **Quitar** y haga clic en **Aplicar** para eliminar la clave existente.

1. Si selecciona la opción **Configurar usuario** y hace clic en **Siguiente**, aparecerá la página **Configuración de usuario.**

2. En la pantalla **Configuración de usuario**, configure las propiedades y los privilegios de usuario.

   La Tabla 5-12 describe los valores **Generales** de configuración de un nombre de usuario y contraseña del iDRAC6.

   La Tabla 5-13 describe los **Privilegios de la LAN de IPMI** para configurar los privilegios de LAN del usuario.

   La Tabla 5-14 describe los permisos del **Grupo** de **usuarios** para la configuración de los **Privilegios de LAN de IPMI** y de los Privilegios de usuario del iDRAC6.

   La Tabla 5-15 describe los permisos de **Grupo de iDRAC6**. Si agrega un **Privilegio de usuario del iDRAC6** al **Administrador**, **Usuario avanzado** o **Usuario invitado**, el **Grupo** de iDRAC6 cambiará a grupo **Personalizado**.

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

4. Para continuar, haga clic en el botón correspondiente. Consulte Tabla 5-16.

Tabla 5-12. 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 del usuario está desactivado.
Nombre de usuario	Especifica un nombre de usuario del iDRAC6 de hasta 16 caracteres. Cada usuario debe tener un nombre de usuario único. **NOTA:** Los nombres de usuarios en el iDRAC6 no pueden incluir los caracteres @,#,$,%,/,. (punto) y distinguen entre mayúsculas y minúsculas. **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. **NOTA:** Caracteres especiales como **<**, **>**, y **** no se admiten y se bloquean al crear contraseñas de usuarios.
Confirmar nueva contraseña	Vuelva a escribir la contraseña del usuario del iDRAC6 para confirmarla.

Tabla 5-13. Privilegio 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 está **seleccionado**, este privilegio está activado.

Tabla 5-14. Otro Privilegio

Propiedad	Descripción
Grupo del iDRAC6	Especifica el privilegio máximo del usuario de iDRAC6 como uno de los siguientes: **Administrador**, **Usuario avanzado**, **Usuario invitado**, **Personalizado** o **Ninguno**. Consulte la Tabla 5-15 para ver los permisos del **Grupo de iDRAC6**.
Iniciar sesión en el iDRAC6	Permite al usuario iniciar sesión en el iDRAC6.
Configurar el iDRAC6	Permite al usuario configurar el iDRAC6.
Configurar usuarios	Activa la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos. **PRECAUCIÓN: La capacidad de cargar, ver y/ o eliminar claves SSH depende del privilegio de usuario "Configurar usuarios". Este privilegio les permite a los usuarios configurar la clave SSH de cualquier otro usuario. Dada la importancia de las claves SSH, otorgue este privilegio con mucho cuidado.**
Borrar registros	Permite al usuario borrar los registros del iDRAC6.
Ejecutar comandos de	Permite al usuario ejecutar comandos de RACADM.

control del servidor	
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 todos los destinatarios de alertas actualmente configurados.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Tabla 5-15. Permisos de grupo del iDRAC6

Grupo de usuarios	Permisos concedidos
Administrador	**Iniciar sesión en el iDRAC6**, **Configurar el iDRAC6**, **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 iDRAC6**, **Borrar registros**, **Ejecutar comandos de control del servidor**, **Acceder a la redirección de consola**, **Acceder a los medios virtuales**, **Probar alertas**
Usuario invitado	**Iniciar sesión en el iDRAC6**
Personalizado	Seleccione cualquier combinación de los permisos siguientes: **Iniciar sesión en el iDRAC6**, **Configurar el iDRAC6**, **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**
Ninguno	Sin permisos asignados

Tabla 5-16. 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 del 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 sockets seguros (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 sockets seguros (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:

- Autenticarse ante un cliente habilitado con SSL
- Permitir que el cliente se autentique ante el servidor
- Permitir 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 del iDRAC6 tiene un certificado digital SSL autofirmado (identificación del servidor) de Dell. Para garantizar una alta seguridad en Internet, sustituya el certificado SSL del servidor web por otro firmado por una entidad de certificación (CA) de renombre. Una entidad de certificación (o entidad emisora de certificado) 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®. 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 solicitud CSR generada a una entidad de certificación 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 permiten a clientes del servidor confiar en la identidad del servidor y negociar una sesión cifrada con el servidor.

Una vez que la autoridad de certificados recibe una solicitud CSR, revisa y verifica la información que contiene. Si el solicitante cumple los estándares de seguridad, la autoridad de certificados 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 que contiene el certificado, es decir, el certificado se tiene que haber generado en respuesta a la CSR creada por el iDRAC6.

Acceso al menú principal de SSL

1. Haga clic en la ficha **Sistema**→ **Acceso remoto**→ **iDRAC6**→ **Red/Seguridad**.
2. Haga clic en **SSL** para abrir la pantalla **SSL**.

La Tabla 5-17 describe las opciones disponibles al momento de generar una CSR.

La Tabla 5-18 describe los botones disponibles en la pantalla **Menú principal de SSL**.

Tabla 5-17. 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 autoridad de certificados acepte la solicitud CSR que usted envíe, la solicitud CSR que está en el firmware debe coincidir con el certificado que devuelve esta entidad.
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 5-18. Botones del menú principal de SSL

Botón	Descripción
Imprimir	Imprime los valores de **SSL** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **SSL**.
Siguiente	Procesa la información de la pantalla **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 **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 5-19 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 CSR en la estación de administración remota.

5. Para continuar, haga clic en el botón correspondiente. Consulte el apartado Tabla 5-20.

Tabla 5-19. Opciones para 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, espacios, guiones, guiones bajos y puntos.
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 organizacional, como un departamento (por ejemplo, Tecnología informática). Sólo son válidos los caracteres alfanuméricos, guiones, guiones bajos, puntos y espacios.
Localidad	Ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Round Rock). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo ni otro carácter.
Nombre del estado	El estado o provincia en el que se ubica la entidad que solicita una certificación (por ejemplo, Texas). 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.
Tamaño de clave	El tamaño de la clave de solicitud de firma de certificado (CSR) que generará. El tamaño puede variar entre 1024 KB ó 2048 KB.

Tabla 5-20. Botones para generar una solicitud de firma de certificado (CSR)

Botón	Descripción
Imprimir	Imprime los valores de **Generar solicitud de firma de certificado (CSR)** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **Generar solicitud de firma de certificado (CSR)**.
Generar	Genera una CSR y luego pide al usuario que la 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 **SSL**.

Carga de un certificado de servidor

1. En la pantalla **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 en la estación de administración.

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. Consulte Tabla 5-21.

Tabla 5-21. 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 pantalla **SSL**, seleccione **Ver certificado del servidor** y haga clic en **Siguiente**.

   La Tabla 5-22 describe los campos asociados con las descripciones que aparecen en la ventana **Ver certificado del servidor**.

2. Para continuar, haga clic en el botón correspondiente. Consulte Tabla 5-23.

Tabla 5-22. Ver información de certificado del servidor

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 5-23. 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 los certificados de Microsoft 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 del servicio de directorio de iDRAC6".

Para acceder a la pantalla Resumen de **Microsoft Active Directory**, haga clic en la ficha **Sistema**→ **Acceso remoto**→ **iDRAC6**→ **Red/Seguridad** → **Servicio de directorios**→ **Microsoft Active Directory**.

La Tabla 5-24 indica las opciones de resumen de **Active Directory**. Para continuar, haga clic en el botón correspondiente.

Tabla 5-24. Opciones de Active Directory

Campo	Descripción
Valores comunes	Muestra configuraciones frecuentes de Active Directory.
Certificado de CA de Active Directory	Muestra el certificado de la CA que firma todos los certificados de servidor SSL del controlador de dominio.
Configuración del esquema estándar/Configuración del esquema ampliado	Según la configuración actual de Active Directory, se muestran la configuración del esquema ampliado o la configuración del esquema estándar.
Configurar Active Directory	Haga clic en esta opción para configurar el paso 1 de 4 de la configuración de Active Directory. La página **Paso 1 de 4 Active Directory** permite cargar un certificado de la autoridad de certificados (CA) de Active Directory al iDRAC6, ver el certificado actual de CA de Active Directory que se cargó al iDRAC6 o activar la validación de certificados.
Probar configuración	Haga clic en esta opción para verificar la configuración de Active Directory con las opciones especificadas.
Cargar keytab de Kerberos	Haga clic en esta opción para cargar un archivo keytab de Kerberos en el iDRAC6. Para obtener información sobre cómo crear un archivo keytab, consulte "Activación de la autentificación con Kerberos".

Tabla 5-25. Botones de Active Directory

Botón	Definición
Imprimir	Imprime los valores de **Active Directory** que aparecen en la pantalla.
Actualizar	Vuelve a cargar la pantalla **Active Directory**.

Configuración de Active Directory (esquema estándar y esquema ampliado)

1. En la pantalla de resumen de **Active Directory**, haga clic en **Configurar Active Directory**.

2. En la pantalla **Paso 1 de 4 Active Directory**, puede activar la validación de certificados, cargar el certificado de CA de Active Directory en el iDRAC6 o ver el certificado de CA de Active Directory actual.

   La Tabla 5-26 describe la configuración y las selecciones para cada paso del proceso de **Configuración y administración de Active Directory**. Para continuar, haga clic en el botón correspondiente.

Tabla 5-26. Valores de configuración de Active Directory

Valor	Descripción
Paso 1 de 4 Configuración y administración de Active Directory	
Validación de certificados activada	Especifica si la validación de certificados está activada o desactivada. Si está **seleccionada**, la validación de certificados está activada. El iDRAC6 usa LDAP sobre la capa de sockets seguros (SSL) mientras se conecta a Active Directory. De manera predeterminada, al usar el certificado de la entidad emisora cargado en el iDRAC6, éste último proporciona una gran seguridad para validar el certificado del servidor SSL de los controladores de dominio durante el protocolo de enlace SSL. La validación de certificados se puede desactivar para fines de prueba.
Cargar un certificado de CA de Active Directory	Para cargar un certificado de la entidad emisora de Active Directory, haga clic en **Examinar**, seleccione el archivo y haga clic en **Cargar**. Asegúrese de que los certificados SSL del controlador de dominio estén firmados por la misma entidad emisora y que el certificado esté disponible en la estación de administración que esté accediendo al iDRAC6. El valor **Ruta de acceso del archivo** muestra la ruta de acceso del archivo del certificado que se va a cargar. Si elige no buscar el certificado, introduzca la ruta de acceso del archivo, incluida la ruta de acceso completa y el nombre y la extensión del archivo completos.
Certificado de CA de Active Directory actual	Muestra el certificado de CA de Active Directory que se cargó al iDRAC6.
Paso 2 de 4 Configuración y administración de Active Directory	
Active Directory activado	Seleccione esta opción si desea activar Active Directory.
Activar inicio de sesión mediante tarjeta inteligente	Seleccione esta opción para activar el inicio de sesión mediante tarjeta inteligente. Se le pedirá el inicio de sesión mediante tarjeta inteligente durante cualquier intento subsiguiente de inicio de sesión mediante la interfaz gráfica de usuario. **NOTA:** Las funciones de autentificación de dos factores (TFA) con tarjeta inteligente e inicio de sesión único sólo se admiten en los sistemas operativos Microsoft Windows con Internet Explorer. Además, los servicios de Terminal Server (escritorio remoto) en Windows XP® no son compatibles con el funcionamiento de la tarjeta inteligente. Sin embargo, Windows Vista® admite esta utilización.
Activar inicio de sesión único	Seleccione esta opción si desea iniciar sesión en el iDRAC6 sin necesidad de introducir credenciales de autentificación de usuario de dominio, por ejemplo, nombre de usuario y contraseña. Si activa el inicio de sesión único (SSO) y luego se desconecta, puede volver a iniciar sesión mediante SSO. Si ya inició sesión a través de SSO y luego se desconectó, o si falló el SSO, se mostrará la página web normal de inicio de sesión. **NOTA:** Activar el inicio de sesión mediante tarjeta inteligente **o** el inicio de sesión único no desactiva ninguna interfaz fuera de banda de línea de comandos, incluidos SSH, Telnet, RACADM remoto e IPMI en la LAN. **NOTA:** Las funciones de autentificación de dos factores (TFA) con tarjeta inteligente e inicio de sesión único (SSO) no pueden utilizarse si Active Directory está configurado para el esquema ampliado.
Nombre de dominio del usuario	Introduzca las anotaciones del nombre de dominio del usuario. Si esta opción está configurada, en la página de inicio de sesión aparecerá una lista de nombres de dominios de usuarios como menú desplegable. Si no está configurado, los usuarios de Active Directory podrán iniciar sesión al introducir el nombre de usuario con el formato nombre_de_usuario@nombre_de_dominio o nombre_de_dominio\nombre_de_usuario. **Agregar**: Añade una nueva anotación de nombre de dominio de usuario a la lista. **Editar**: Modifica una anotación existente de nombre de dominio de usuario. **Eliminar**: Elimina una anotación de la lista de nombre de dominio de usuario.
Tiempo de espera	Introduzca el tiempo máximo (en segundos) de espera para que terminen las consultas a Active Directory.
Buscar controladores de dominio con DNS	Seleccione la opción **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory de una búsqueda en el DNS. Al seleccionar esta opción, se ignoran las direcciones 1-3 del servidor del controlador de dominio. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. De lo contrario, seleccione la opción **Especificar un dominio** y escriba el nombre de dominio para usar en la búsqueda en el DNS. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión exitosa. Si se selecciona el **esquema ampliado**, los controladores de dominio se encuentran donde están ubicados el objeto dispositivo iDRAC6 y los objetos de asociación. Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.
Especificar direcciones del controlador de dominio	Seleccione la opción **Especificar direcciones del controlador de dominio** para que el iDRAC6 pueda usar las direcciones especificadas del servidor del controlador de dominio de Active Directory. Al seleccionar esta opción, no se realiza la búsqueda en DNS. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Al seleccionar la opción **Especificar direcciones del controlador de dominio**, es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión exitosa. Si la opción **Esquema estándar** está seleccionada, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones. Si la opción **Esquema ampliado** está seleccionada, las direcciones representan los controladores de dominio donde se encuentran el objeto dispositivo iDRAC6 y los objetos de asociación.
Paso 3 de 4 Configuración y administración de Active Directory	
Selección de esquema ampliado	Seleccione esta opción si desea usar el esquema ampliado con Active Directory. Haga clic en **Siguiente** para mostrar la página **Paso 4 de 4 Configuración y administración de Active Directory**. **Nombre del iDRAC6**: Especifica el nombre que identifica de manera exclusiva el iDRAC6 en Active Directory. De manera predeterminada, este valor es NULO. **Nombre de dominio del iDRAC6**: El nombre de DNS (cadena) del dominio donde reside el objeto del iDRAC de Active Directory. De manera predeterminada, este valor es NULO. Estos valores sólo aparecen si el iDRAC fue configurado para utilizarse con el esquema ampliado de Active Directory.
Selección de	Seleccione esta opción si desea usar esquema estándar con Active Directory.

esquema estándar	Haga clic en **Siguiente** para mostrar la página **Paso 4a de 4 de Active Directory**. Seleccione la opción **Buscar servidores del catálogo global con DNS** y escriba el **Nombre de dominio raíz** para usar en una búsqueda en el DNS y obtener los servidores de catálogo global de Active Directory. Al seleccionar esta opción, se ignoran las **direcciones 1-3 del servidor del catálogo global**. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión exitosa. El servidor de catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. Seleccione la opción **Especificar direcciones del servidor del catálogo global** y escriba la dirección IP o el nombre de dominio completo (FQDN) del/de los servidor(es) del catálogo global. Al seleccionar esta opción, no se realiza la búsqueda en DNS. Al menos una de las tres direcciones debe estar configurada. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión exitosa. El servidor de catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. **Grupos de funciones :** Especifica la lista de grupos de función asociados al iDRAC6. **Nombre de grupo:** Especifica el nombre que identifica el grupo de funciones en Active Directory relacionado con el iDRAC6. **Dominio del grupo**: Especifica el tipo de dominio del grupo donde reside el grupo de funciones. **Privilegios de grupo de funciones**: Especifica el nivel de privilegio del grupo. (vea la Tabla 5-27). Estos valores sólo aparecerán si el iDRAC6 fue configurado para usarse con el esquema estándar de Active Directory.

Tabla 5-27. 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 5-28 para ver los permisos del **Grupo de funciones.**
Iniciar sesión en el iDRAC6	Permite que el grupo inicie sesión en el iDRAC6.
Configurar el iDRAC6	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 5-28. Permisos del grupo de funciones

Propiedad	Descripción
Administrador	Iniciar sesión en el iDRAC6, Configurar el iDRAC6, 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 iDRAC6, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la redirección de consola, Acceder a los medios virtuales, Probar alertas
Usuario invitado	Iniciar sesión en el iDRAC6
Personalizado	Seleccione cualquier combinación de los permisos siguientes: Iniciar sesión en el iDRAC6, Configurar el iDRAC6, 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
Ninguno	Sin permisos asignados

Cómo ver un certificado de CA de Active Directory

En la página de resumen **Active Directory**, haga clic en **Configurar Active Directory** y luego haga clic en **Siguiente**. Se muestra la sección **Certificado de CA de Active Directory actual**. Consulte el apartado Tabla 5-29.

Tabla 5-29. Información del certificado de CA de Active Directory

Campo	Descripción
Número de serie	El número de serie del certificado.
Información del titular	Los atributos del certificado introducidos por el titular.

Información del emisor	Los atributos del certificado generados por el emisor.
Válido desde	La fecha de emisión del certificado.
Válido hasta	La fecha de expiración del certificado.

Activación 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**→ **iDRAC6**→ **Red/Seguridad**→ **Servicios**.
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**.

Desactivación del acceso a la configuración local

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC6**→ **Red/Seguridad**→ **Servicios**.
2. En **Configuración local**, haga clic para seleccionar la casilla **Desactivar actualizaciones de Configuración de USUARIO iDRAC6 local** para desactivar el acceso.
3. Haga clic en **Aplicar**.

Configuración de los servicios del iDRAC6

NOTA: Para modificar esta configuración, debe contar con permiso para **Configurar el iDRAC6**.

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

NOTA: Existe un problema conocido con el cliente Telnet suministrado con Microsoft Windows. Use otro cliente Telnet como HyperTerminal o PuTTY.

1. Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC6** y 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 5-30 para ver la configuración del servidor web
   - SSH: Consulte la Tabla 5-31 para ver la configuración de SSH
   - Telnet: Consulte la Tabla 5-32 para ver la configuración de Telnet
   - 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**.

Tabla 5-30. Configuración del servidor Web

Valor	Descripción
Activado	Activa o desactiva el servidor web del iDRAC6. Cuando está **seleccionado**, indica que el servidor web está activado. El valor predeterminado es **seleccionado**.
Máx. de sesiones	El número máximo de sesiones del servidor web simultáneas que se permite para este sistema. Este campo no se puede editar. Puede haber 4 sesiones simultáneas del servidor web.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **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 de 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 HTTPS	El puerto en el que el iDRAC6 espera una conexión de explorador segura. El valor predeterminado es **443**.

Tabla 5-31. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Cuando está **seleccionada**, la casilla indica que SSH está activado.
Máx. de sesiones	El número máximo de sesiones SSH simultáneas que se permite para este sistema. Se admiten 4 sesiones SSH simultáneas. No puede editar este campo.
Sesiones activas	El número de sesiones actuales en el sistema. No puede editar este campo.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango de 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 5-32. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando está **seleccionado**, Telnet está activado. El valor predeterminado es **deseleccionado**.
Máx. de sesiones	El número máximo de sesiones simultáneas Telnet que se permite para este sistema. Se admiten 4 sesiones Telnet simultáneas. No puede editar este campo.
Sesiones activas	El número actual de sesiones Telnet en el sistema. No puede editar este campo.
Tiempo de espera	El tiempo de espera en inactividad de Telnet, en segundos. El rango de 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 5-33. Agente de recuperación automática del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automática del sistema.

Actualización del firmware de iDRAC6

NOTA: Si el firmware del iDRAC6 se daña, como puede suceder cuando la actualización del firmware del iDRAC6 se interrumpe antes de terminar, puede recuperar el iDRAC6 por medio del CMC. Consulte la *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 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**→ **iDRAC6** y 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 ventana **Actualización del firmware: Cargar (página 1 de 4)**, haga clic en **Examinar** y seleccione la imagen del firmware.

   Por ejemplo:

   `C:\Updates\V2.1\<nombre_de_imagen>`.

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

4. Haga clic en **Cargar**. El archivo se cargará en el iDRAC6. Este proceso podría tardar varios minutos.
5. En la página **Cargar (paso 2 de 4)**, verá los resultados de la validación realizada sobre el archivo de imagen que usted cargó.
   - Cuando el archivo de imagen se cargue correctamente y pase todas las revisiones de verificación, aparecerá un mensaje que indicará que la

imagen del firmware ha sido verificada.

- Si la imagen no se cargó correctamente, ni pasó las revisiones de verificación, restablezca el iDRAC6, cierre le sesión actual y luego intente actualizar nuevamente.

NOTA: Si deja en blanco 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.

6. 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, deje en blanco la casilla de verificación **Conservar configuración**.

7. En la ventana **Actualización (Paso 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**.

8. 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. Para continuar accediendo al iDRAC6 a través de la interfaz web, cierre la ventana actual del explorador y vuelva 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 o RACADM del CMC para actualizar el firmware del iDRAC6. Esta función está disponible cuando el firmware del iDRAC6 está en modo Normal y cuando está dañado.

NOTA: Consulte la *Guía del usuario de firmware de 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 más reciente del iDRAC6 a la estación de administración en **support.dell.com**.

2. Inicie sesión en la interfaz web del CMC.

3. Haga clic en **Chasis** en el árbol del sistema.

4. Haga clic en la ficha **Actualizar**. Aparecerá la pantalla **Actualización del firmware**.

5. Seleccione el iDRAC6 o los iDRAC6 del mismo modelo a actualizar. Para ello, seleccione la casilla **Actualizar destinos**.

6. Haga clic en el botón **Aplicar actualización del iDRAC6 Enterprise** debajo de la lista componentes del iDRAC6.

7. Haga clic en **Examinar**, busque la imagen del firmware del iDRAC6 que descargó y haga clic en **Abrir**.

8. Haga clic en **Iniciar actualización del firmware**.

Después de que el archivo de imagen del firmware haya sido cargado en el CMC, el iDRAC6 se actualizará con la imagen.

Reversión del firmware del iDRAC6

iDRAC6 es capaz de mantener dos imágenes de firmware simultáneamente. Puede optar por iniciar desde la imagen de firmware de su elección o revertir el firmware a dicha imagen.

1. Abra la interfaz web del iDRAC6 e inicie sesión en el sistema remoto.

   Haga clic en **Sistema→ Acceso remoto→ iDRAC6** y luego haga clic en la ficha **Actualizar**.

2. Haga clic en **Revertir**. Las versiones de firmware actuales y anteriores se muestran en la página **Revertir (Paso 2 de 3)**.

3. Haga clic en **Siguiente** para iniciar el proceso de reversión de firmware.

   En la página **Revertir (Paso 3 de 3)**, se mostrará el estado de la operación de reversión. Una vez que se haya completado correctamente, se muestra que el proceso se completó satisfactoriamente.

   Si la reversión del firmware es correcta, el iDRAC se restablecerá automáticamente. Para continuar trabajando con el iDRAC6 por medio de la interfaz web, cierre la ventana actual del explorador y vuelva a conectarse al iDRAC6 desde una ventana nueva del explorador. Se muestra un mensaje de error si ocurre uno.

   NOTA: La función **Conservar configuración** no funciona si desea revertir el firmware del iDRAC6 de la versión 2.2 a la versión 2.1.

Regresar a la página de contenido

Regresar a la página de contenido

Uso del servicio de directorio de iDRAC6

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Un servicio de directorio mantiene una base de datos común para almacenar información acerca de usuarios, equipos, impresoras, etc. en una red. Si la empresa utiliza el software de servicio Microsoft® Active Directory® o el servicio de directorio LDAP, puede configurarlo para que proporcione acceso al iDRAC6, lo que le permite agregar privilegios de usuario del iDRAC6 a los usuarios existentes y controlar estos privilegios en su servicio de directorio.

Uso del iDRAC6 con Microsoft 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 privilegios de usuario de Active Directory del iDRAC6.

Tabla 6-1. Privilegios de usuario del iDRAC6

Privilegio	Descripción
Iniciar sesión en el iDRAC6	Permite al usuario iniciar sesión en el iDRAC6.
Configurar el iDRAC6	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 del 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.

Prerrequisitos 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 autenticar 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 sockets seguros (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 autentificación compatibles de Active Directory

Puede utilizar Active Directory para definir el acceso de los usuarios en el iDRAC6 mediante dos métodos: Por medio de la solución de *esquema extendido* que Dell ha personalizado para agregar objetos de Active Directory definidos por Dell. También puede usar la solución de *esquema estándar*, que utiliza únicamente objetos de grupo de Active Directory. Consulte las siguientes secciones para obtener más información sobre estas soluciones.

Cuando se usa Active Directory para configurar el acceso al iDRAC6, se debe elegir la solución del esquema extendido o la del esquema estándar.

Las ventajas de usar la solución de esquema extendido 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 extensión 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 extendido de Active Directory

Para utilizar la solución de esquema extendido, es necesario una extensión del esquema de Active Directory, según se describe en la siguiente sección.

Extensión del esquema de Active Directory

Importante: La extensión del esquema para este producto es distinta de la de generaciones anteriores de productos de Dell Remote Management. Deberá extender 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 extensión del nuevo esquema y la instalación de la nueva extensión 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 extensión del 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 extensión 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 cree objetos de asociación o de dispositivo iDRAC6, seleccione **Dell Remote Management Object Advanced**.

Extensiones de esquema de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase 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 extender la base de datos de Active Directory al agregar sus propios atributos y clases exclusivos para solucionar las necesidades específicas del entorno. Dell ha extendido el esquema para incluir los cambios necesarios para admitir la autentificación y autorización de administración remota.

Cada atributo o clase que se agrega a un esquema existente de Active Directory debe ser definida con una identificación única. Para mantener identificaciones únicas a través de la industria, Microsoft mantiene una base de datos de Identificadores de Objeto de Active Directory (OID) de modo que cuando las compañías agregan extensiones al esquema, se pueda garantizar que serán únicas y no entrarán en conflicto una con otra. Para extender 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`
- El OID base de Dell 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 extendido 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 iDRAC6. Este modelo proporciona máxima flexibilidad al administrador con respecto a las diferentes combinaciones de usuarios, privilegios del iDRAC6 y dispositivos 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 iDRAC6. Puede crear varios objetos de asociación y cada uno de ellos puede vincularse a cuantos usuarios, grupos de usuarios u objetos de dispositivo iDRAC6 sean necesarios. 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 es posible que vincule usuarios, grupos de usuarios u objetos de dispositivo 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 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 autentificaciones y autorizaciones.

Figura 6-1. Configuración típica de los objetos de Active Directory

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 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 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* en 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.

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

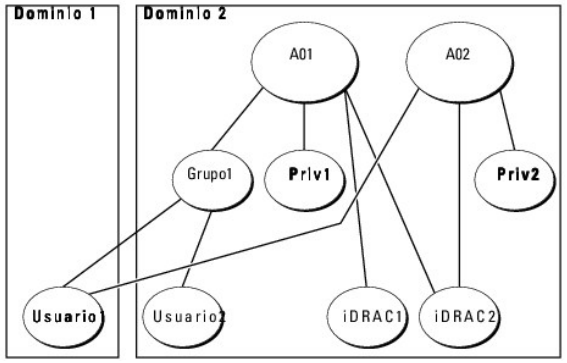
Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio pueden agregarse al objeto de asociación. Las soluciones de esquema extendido admiten todo tipo de grupos de usuarios o todo grupo anidado de usuarios en varios dominios permitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema extendido

El mecanismo de autentificación del esquema extendido 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 autentificación del esquema extendido 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 extendido.

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 el iDRAC2.

Por ejemplo, Priv1 tiene los privilegios: Inicio de sesión, Medios virtuales y Borrar registros; mientras que 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 extendido 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 extendido 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. Extienda el esquema de Active Directory (consulte "Extensión del esquema de Active Directory").

2. Extienda 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 Microsoft Active Directory con esquema extendido por medio de la interfaz web del iDRAC6" o "Configuración de Active Directory con esquema extendido por medio de RACADM").

La extensión del esquema de Active Directory agrega una unidad organizacional Dell, clases y atributos de esquema, así como privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender 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 extender el esquema por medio de uno de los siguientes métodos:

- 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 léame que está en el directorio **LDIF_Files**. Para usar Dell Schema Extender para extender el esquema de Active Directory, consulte "Uso de Dell Schema Extender".

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

Uso de Dell Schema Extender

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 Dell Schema Extender.

5. Haga clic en **Terminar**.

   El esquema ha sido extendido. Para verificar la extensión 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
Superclases	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
Superclases	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
Superclases	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
Superclases	Usuario
Atributos	**dellRAC4Privileges**

Tabla 6-7. Clase dellProduct

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
Superclases	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 dellPrivilege que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers Lista 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 distintivo (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 dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena en que se ignoran las mayúsculas (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 Cadena en que se ignoran las mayúsculas (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 distintivo (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 extiende el esquema en Active Directory, también debe extenderse 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, así como las asociaciones y privilegios del iDRAC6.

Cuando instala el software de administración de sistemas con el DVD **Dell Systems Management Tools and Documentation**, puede extender 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 del paquete de administrador

Debe instalar el paquete de administrador en cada sistema que administre los objetos iDRAC6 de Active Directory. Si no lo hace, no podrá ver el objeto iDRAC6 de Dell en el contenedor.

Consulte "Cómo abrir el complemento Usuarios y equipos de Active Directory" para obtener más información.

Cómo abrir el complemento Usuarios y equipos de Active Directory

Para 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 **Complemento de usuarios y equipos de Active Directory** y haga clic en **Agregar**.

5. Haga clic en **Cerrar** y luego en **Aceptar**.

Cómo agregar usuarios y privilegios del iDRAC6 a Active Directory

El complemento de usuarios y equipos de Active Directory extendido 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 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 iDRAC6

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. El nombre debe ser idéntico al nombre del iDRAC6 que va a introducir en el Paso A de "Configuración de Microsoft Active Directory con esquema extendido por medio de la interfaz web del iDRAC6".

4. Seleccione Objeto de dispositivo i**DRAC**.

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 Tabla 5-14).

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 iDRAC6 o grupos de dispositivos 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 Microsoft Active Directory con esquema extendido por medio de la interfaz 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**→ **iDRAC6**→ ficha **Red/Seguridad** → **Servicio de directorio**→ **Microsoft Active Directory**.

   Aparece la pantalla de resumen de **Active Directory**.

4. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

   Aparece la pantalla **Paso 1 de 4 Active Directory**.

5. Para validar el certificado SSL de los servidores Active Directory, seleccione la casilla **Validación de certificados activada** en **Configuración de certificados**.

   Si no desea validar el certificado SSL de los servidores Active Directory, vaya al paso 7.

6. En **Cargar 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 para el certificado de la entidad emisora de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.

7. Haga clic en **Siguiente**.

   Aparece la pantalla **Paso 2 de 4 de Configuración y administración de Active Directory**.

8. Seleccione la casilla **Active Directory activado**.

   NOTA: En esta versión, las funciones de autenticación en dos fases (TFA) con tarjeta inteligente e inicio de sesión único (SSO) no pueden utilizarse si Active Directory está configurado para el **esquema extendido**.

9. Haga clic en **Agregar** para introducir el **Nombre de dominio de usuario**. Introduzca el nombre del dominio en el campo de texto y luego 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 en la interfaz web. Puede elegir de la lista y luego sólo debe ingresar el nombre de usuario.

10. En el campo **Tiempo de espera,** ingrese la cantidad de segundos que desea que el iDRAC6 espere las respuestas de Active Directory.

11. Seleccione la opción **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory de una búsqueda en el DNS. Si ya están configuradas, las **Direcciones 1 a 3 del servidor del controlador de dominio** se ignoran. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. De lo contrario, seleccione la opción **Especificar un dominio** y escriba el nombre de dominio para usar en la búsqueda en el DNS. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión exitosa. Si se selecciona el **esquema extendido**, los controladores de dominio se encuentran donde están ubicados el objeto dispositivo iDRAC6 y los objetos de asociación. Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.

    NOTA: iDRAC6 no cuenta con protección contra fallas para los controladores de dominio especificados cuando falla la búsqueda en el DNS, pues de ser así ninguno de los servidores que ofrece la búsqueda en el DNS funciona.

12. Seleccione la opción **Especificar direcciones del controlador de dominio** para que el iDRAC6 pueda usar las direcciones especificadas del servidor del controlador de dominio de Active Directory. La búsqueda en el DNS no se realizó. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Al seleccionar la opción **Especificar direcciones del controlador de dominio**, es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión exitosa. Si la opción **Esquema extendido** está seleccionada, las direcciones representan los controladores de dominio donde se encuentran el objeto dispositivo iDRAC6 y los objetos de asociación.

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.

13. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 3 de 4 de Configuración y administración de Active Directory**.

14. En **Selección de esquema**, seleccione la casilla **Selección de esquema extendido.**

15. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 4 de 4 de Active Directory**.

16. En **Configuración del esquema extendido**, introduzca el **Nombre del iDRAC6** y el **Nombre de dominio del iDRAC6** para configurar el objeto de dispositivo iDRAC6 y su ubicación en Active Directory.

17. Haga clic en **Terminar** para guardar los cambios y luego en **Terminado**.

    Aparece la página principal de resumen **Configuración y administración de Active Directory**. A continuación, pruebe los valores de Active Directory que ha configurado.

18. Desplácese hasta la parte inferior de la pantalla y haga clic en **Probar configuración.**

    Aparece la pantalla **Probar configuración de Active Directory**.

19. Ingrese su nombre de usuario y contraseña del iDRAC6 y luego haga clic en **Iniciar prueba**.

    Se mostrarán los resultados de la prueba 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 **Red** (haga clic en **Sistema→ Acceso remoto→ iDRAC6** y luego haga clic en **Red/Seguridad→** ficha **Red**) para configurar los servidores DNS de forma manual o usar DHCP para obtener los servidores DNS.

Con este paso se completa la configuración de Active Directory con esquema extendido.

Configuración de Active Directory con esquema extendido por medio de RACADM

Use los siguientes comandos para configurar la función de Active Directory del iDRAC6 con esquema extendido por medio de la herramienta de interfaz de línea de comandos (CLI) de RACADM en lugar de la interfaz web.

1. Abra un símbolo del sistema y escriba los siguientes comandos de RACADM:

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

   racadm config -g cfgActiveDirectory -o cfgADType 1

   racadm config -g cfgActiveDirectory -o
   cfgADRacName <nombre común de RAC>

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

   racadm config -g cfgActiveDirectory -o cfgADDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgADDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgADDomainController3 <nombre de dominio completo o dirección IP del controlador de dominio>
   ```

   NOTA: Debe configurar por lo menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión exitosa. En el esquema extendido, 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 extendido.

   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 entidad emisora.

   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 la entidad emisora con el siguiente comando de RACADM:

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

   El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "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 del DNS primario>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP del DNS secundario>
```

4. Si desea configurar una lista de dominios de usuario para que solamente tenga que introducir el nombre de usuario cuando se inicia sesión en la interfaz web del iDRAC6, escriba el siguiente comando:

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName <nombre de dominio completo o dirección IP del controlador de dominio> -i <índice>
   ```

   Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

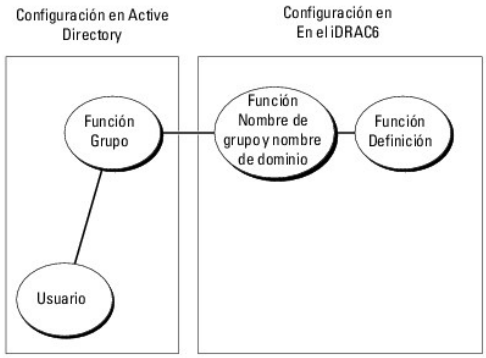
   Consulte "Uso de Active Directory para iniciar sesión en el iDRAC6" para obtener información sobre dominios de usuario.

5. Oprima **Entrar** para completar la configuración de Active Directory con esquema extendido.

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 extendido, 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	Ninguno	**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	Ninguno	**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	Ninguno	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, pertenecen a 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 web o RACADM (consulte "Configuración de Active Directory con esquema estándar mediante la interfaz 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.

Configuración de Active Directory con esquema estándar mediante la interfaz 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**→ **iDRAC6**→ ficha **Red/Seguridad** → **Servicio de directorio**→ **Microsoft Active Directory**.

   Aparece la página de resumen de **Active Directory**.
4. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

   Aparece la pantalla **Paso 1 de 4 Active Directory**.
5. En **Configuración de certificados**, seleccione **Validación de certificados activada**.
6. En **Cargar 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 para el certificado de la entidad emisora de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.
7. Haga clic en **Siguiente**.

   Aparece la pantalla **Paso 2 de 4 de Configuración y administración de Active Directory**.
8. Seleccione la casilla **Active Directory activado**.
9. Seleccione la opción **Activación de inicio de sesión con tarjeta inteligente** para activar el inicio de sesión con tarjeta inteligente. Se le pedirá el inicio de sesión mediante tarjeta inteligente durante cualquier intento subsiguiente de inicio de sesión mediante la interfaz gráfica para usuario.
10. Seleccione **Habilitar inicio de sesión único** si desea iniciar sesión en el iDRAC6 sin necesidad de introducir credenciales de autentificación de usuario de dominio, por ejemplo, nombre de usuario y contraseña.
11. Haga clic en **Agregar** para introducir el **Nombre de dominio de usuario**. Introduzca el nombre del dominio en el campo de texto y luego 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 en la interfaz web. 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 espere las respuestas de Active Directory.
13. Seleccione la opción **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory de una búsqueda en el DNS. Si ya están configuradas, las **Direcciones 1 a 3 del servidor del controlador de dominio** se ignoran. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. De lo contrario, seleccione la opción **Especificar un dominio** y escriba el nombre de dominio para usar en la búsqueda en el DNS. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión exitosa. Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.
14. Seleccione la opción **Especificar direcciones del controlador de dominio** para que el iDRAC6 pueda usar las direcciones especificadas del servidor del controlador de dominio de Active Directory. La búsqueda en el DNS no se realizó. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Al seleccionar la opción **Especificar direcciones del controlador de dominio**, es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión exitosa. Si la opción

esquema estándar está seleccionada, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

NOTA: iDRAC6 no cuenta con protección contra fallas para los controladores de dominio especificados cuando falla la búsqueda en el DNS, pues de ser así ninguno de los servidores que ofrece la búsqueda en el DNS funciona.

15. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 3 de 4 de Configuración y administración de Active Directory**.

16. En **Selección de esquema**, seleccione la casilla **Selección de esquema estándar.**

17. Haga clic en **Siguiente**.

    Aparece la pantalla **Paso 4a de 4 de Active Directory**.

18. En **Configuración del esquema estándar**, seleccione la opción **Buscar servidores del catálogo global con DNS** y escriba el **Nombre de dominio raíz** para usar en una búsqueda en el DNS y obtener los servidores de catálogo global de Active Directory. Si ya están configuradas, las Direcciones 1 a 3 del servidor de Catálogo global se ignoran. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión exitosa. El servidor de catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios.

    NOTA: iDRAC6 no cuenta con protección contra fallas para los servidores de catálogo global especificados cuando falla la búsqueda en el DNS, pues de ser así ninguno de los servidores que ofrece la búsqueda en el DNS funciona.

19. Seleccione la opción **Especificar direcciones del servidor de catálogo global** y escriba la dirección IP o el nombre de dominio completo (FQDN) de los servidores de catálogo global. La búsqueda en el DNS no se realizó. Es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión exitosa.

NOTA: El servidor de catálogo global sólo es necesario 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. Si usa la interfaz gráfica web del iDRAC6 para configurar Active Directory, deberá introducir una dirección global aun si el usuario y el grupo pertenecen al mismo dominio.

20. 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**.

21. Ingrese el **nombre del grupo**. El nombre del grupo identifica el grupo de funciones en Active Directory asociado con el iDRAC6.

22. Ingrese el **dominio del grupo**. El **Nombre de grupo** es el nombre completo del dominio raíz para el bosque.

23. En la sección **Privilegios del grupo de funciones**, defina los privilegios del grupo. Consulte Tabla 5-14 para obtener información sobre los privilegios del grupo 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.

24. 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**.

25. Para agregar un grupo de funciones adicional, repita los pasos paso 20 a paso 24.

26. Haga clic en **Terminar** y luego en **Terminado**.

    Aparece la pantalla principal de resumen **Configuración y administración de Active Directory**. Pruebe los valores de Active Directory que ha configurado.

27. Desplácese hasta la parte inferior de la pantalla y haga clic en **Probar configuración.**

    Aparece la pantalla **Probar configuración de Active Directory**.

28. Ingrese su nombre de usuario y contraseña del iDRAC6 y luego haga clic en **Iniciar prueba**.

    Se mostrarán los resultados de la prueba 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 **Red** (haga clic en **Sistema→ Acceso remoto→ iDRAC6** y luego en **Red / Seguridad→** ficha **Red**) para configurar los servidores DNS de forma manual o usar 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 Active Directory del iDRAC6 con esquema estándar por medio de la interfaz de línea de comandos de RACADM en lugar de la interfaz web.

1. Abra un símbolo del sistema y escriba los siguientes comandos de RACADM:

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

   racadm config -g cfgActiveDirectory -o cfgADType 2

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

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

   racadm config -g cfgStandardSchema -i <indice> -o
   cfgSSADRoleGroupPrivilege <Valor de máscara de bits para
   permisos de grupos de funciones específicos>
   ```

   NOTA: Para conocer los valores de máscara de bits para permisos de grupos de funciones específicos, consulte la Tabla 6-9.

   ```
   racadm config -g cfgActiveDirectory -o cfgADDomainController1 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgADDomainController2 <nombre de dominio completo o dirección IP del controlador de dominio>

   racadm config -g cfgActiveDirectory -o cfgADDomainController3 <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, una por una, 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 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 entidad emisora con el siguiente comando de RACADM:

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

El siguiente comando de RACADM es opcional. Para obtener información adicional, consulte "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 del DNS primario>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <dirección IP del DNS secundario>
   ```

4. Si desea configurar una lista de dominios de usuario para que solamente tenga que introducir el nombre de usuario cuando se inicia sesión en la

interfaz web, escriba el siguiente comando:

```
racadm config -g cfgUserDomain -o cfgUserDomainName <nombre de dominio completo o dirección IP del controlador de dominio> -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 web del iDRAC6.

Una vez definida la configuración en la interfaz web del iDRAC6, haga clic en **Probar configuración** en la parte inferior de la pantalla. Deberá introducir 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 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 CA 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 la entidad emisora 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/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 mouse, 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 14 en el iDRAC6.

    Para cargar el certificado por medio de RACADM, consulte "Configuración de Active Directory con esquema estándar vía RACADM".

    Para cargar el certificado desde la interfaz web, consulte "Configuración de Active Directory con esquema estándar mediante la interfaz web del iDRAC6".

Importar el certificado SSL de firmware del iDRAC6

NOTA: Si el servidor de Active Directory está configurado para autentificar el cliente durante la fase de inicialización de una 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 autentificación de cliente durante la fase de inicio 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 entidad emisora reconocida y dicho certificado ya se encuentra en la lista de certificados de entidad emisora raíz de confianza 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 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**→ **Entidades emisoras raíz de confianza**.

2. Haga clic con el botón derecho del mouse en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.

3. Haga clic en **Siguiente** y desplácese al archivo de certificado SSL.

4. Instale el certificado SSL del iDRAC6 en la lista de **Entidades emisoras raíz de confianza** de cada controlador de dominio.

   Si ha instalado su propio certificado, asegúrese que la CA que firma el certificado esté en la lista **Entidades emisoras raíz de confianza**. Si la autoridad no está en la lista, debe instalarla en todos los controladores de dominio.

5. Haga clic en **Siguiente** y especifique si desea que Windows seleccione automáticamente el almacén de certificados basándose en el tipo de certificado, o examine hasta encontrar 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 web
- RACADM local
- SSH o consola Telnet para la interfaz de línea de comandos 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 web y ha configurado dominios de usuario, aparecerá en pantalla 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 introducir 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."

Uso del inicio de sesión único de Active Directory

Puede configurar el iDRAC6 para utilizar el protocolo de autentificación de red Kerberos a fin de activar el inicio de sesión único. Para obtener más información sobre cómo configurar el iDRAC6 para usar esta función, consulte "Activación de la autentificación con Kerberos".

Configuración del iDRAC6 para usar el inicio de sesión único

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**→ **iDRAC6**→ ficha **Red/Seguridad**→ **Red**. Seleccione la página **Red** y verifique si el **Nombre del iDRAC6 en el DNS** es correcto y coincide con el nombre usado para nombres de dominio completos del iDRAC6.
4. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC6**→ ficha **Red/Seguridad** → **Servicio de directorio**→ **Microsoft Active Directory**.

   Aparece la pantalla de resumen 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 Active Directory**.
6. Para validar el certificado SSL de los servidores Active Directory, seleccione la casilla **Validación de certificados activada** en **Configuración de certificados**.

   Si no desea validar el certificado SSL de los servidores Active Directory, no realice ninguna acción; proceda a paso 7.
7. En **Cargar 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 para el certificado de la entidad emisora 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 de Configuración y administración de Active Directory**.
9. Seleccione la casilla **Active Directory activado**.
10. Seleccione **Habilitar inicio de sesión único** si desea iniciar sesión en el iDRAC6 directamente después de conectar la estación de trabajo sin necesidad de introducir credenciales de autentificación de usuario de dominio, por ejemplo, nombre de usuario y contraseña.

    Para iniciar sesión en el iDRAC6 por medio de esta función, es necesario haber iniciado sesión en el sistema por medio de una cuenta de usuario de Active Directory válida. Además, también se requiere haber configurado la cuenta de usuario para iniciar sesión en el iDRAC6 por medio de las credenciales de Active Directory. El iDRAC6 utiliza las credenciales de Active Directory guardadas en la caché para permitir el inicio de sesión.

    Para activar la función de inicio de sesión único por medio de CLI, ejecute el siguiente comando RACADM:

    ```
    racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
    ```
11. Agregue el **nombre de dominio del usuario** e introduzca la dirección IP de la dirección de servidor del controlador de dominio. Seleccione la opción **Buscar controladores de dominio con DNS** o la opción **Especificar direcciones del controlador de dominio**. Seleccione **Siguiente**.
12. Seleccione **Configuración del esquema estándar** en la página **Paso 3 de 4 Configuración y administración de Active Directory**. Seleccione **Siguiente**.
13. En la página **4a de 4 de Active Directory**, escriba la dirección IP del **Servidor de catálogo global** o seleccione la opción **Buscar servidores de catálogo global con DNS** y escriba el **Nombre de dominio raíz** para realizar una búsqueda en el DNS y obtener los servidores de catálogo global activos. Agregue la información de grupo de funciones del cual es miembro su usuario válido de Active Directory; para ello, seleccione uno de los grupos de funciones (*Paso 4B de 4*). Introduzca el nombre del grupo de funciones, el dominio del grupo y los niveles de privilegio del grupo de funciones. Seleccione **Aceptar** y luego **Terminar**. Seleccione **Listo** para mostrar la página de resumen de **Active Directory**.

Inicio de sesión en el iDRAC6 mediante inicio de sesión único

1. Inicie sesión en la estación de administración mediante su cuenta de red de Active Directory válida.
2. Inicie sesión en la página web del iDRAC6 mediante el nombre de dominio completo del iDRAC6:

   http://nombre_del_idrac.dominio.com.

El iDRAC6 iniciará su sesión por medio de las credenciales que quedaron almacenadas en caché en el sistema operativo cuando inició sesión con una cuenta de red válida de Active Directory.

Uso de iDRAC6 con el servicio de directorio LDAP

iDRAC6 ofrece una solución genérica para admitir la autentificación basada en el protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP). Esta función no requiere una extensión del esquema en sus servicios de directorios.

Para que la implementación del LDAP en iDRAC6 sea genérica, se utilizan las características en común de distintos servicios de directorios para agrupar a los usuarios y asignar la relación usuario-grupo. La acción específica del servicio de directorio es el esquema. Por ejemplo, pueden tener distintos nombres de atributo para el grupo, el usuario y el vínculo entre el usuario y el grupo. Estas acciones se pueden configurar en iDRAC6.

Sintaxis de inicio de sesión (usuario de directorio y usuario local)

A diferencia de Active Directory, no se utilizan caracteres especiales ("@", "\", y "/") para diferenciar un usuario LDAP de un usuario local. El usuario que inicia sesión debe ingresar el nombre de usuario, excluyendo el nombre de dominio. iDRAC6 toma el nombre de usuario tal cual se indica y no lo desglosa en nombre de usuario y dominio del usuario. Cuando se activa el LDAP genérico, iDRAC6 primero intenta conectar al usuario como usuario de directorio. Si esto falla, se activa la búsqueda de usuario local.

NOTA: No hay modificación de comportamiento en la sintaxis de inicio de sesión de Active Directory. Cuando se activa el LDAP genérico, la página de inicio de sesión de GUI muestra únicamente la opción **Este iDRAC** en el menú desplegable.

NOTA: En esta versión, sólo están admitidos los servicios de directorio basados en openLDAP y openDS. No están permitidos los caracteres "<" y ">" en el nombre de usuario de openLDAP y OpenDS.

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web de iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Expanda el árbol del **sistema** y haga clic en **Acceso remoto**→ **iDRAC6**→ ficha **Red/Seguridad** → **Servicio de directorio**→ **Servicio de directorio LDAP genérico**.
4. La página **Configuración y administración de LDAP genérico** muestra la configuración actual del LDAP genérico de iDRAC6. Desplácese hasta el final de la página **Configuración y administración de LDAP genérico** y haga clic en **Configurar LDAP genérico**.

   NOTA: En esta versión, sólo se admite Active Directory de esquema estándar (SSAD) sin extensiones.

   Aparece la página **Paso 1 de 3** de **Configuración y administración de LDAP genérico**. Use esta página para configurar el certificado digital que se utiliza durante el inicio de las conexiones de SSL al comunicarse con un servidor LDAP genérico. Estas comunicaciones usan el LDAP a través de SSL (LDAPS). Si activa la convalidación de certificados, cargue el certificado de la Autoridad de certificados (CA) que emitió el certificado utilizado por el servidor LDAP durante el inicio de las conexiones de SSL. El certificado de CA se usa para convalidar la autenticidad del certificado proporcionado por el servidor LDAP durante el inicio de SSL.

   NOTA: En esta versión, no se admite el enlace al LDAP basado en puertos distintos a SSL. Sólo se admite el LDAP a través de SSL.

5. En **Configuración de certificados**, seleccione **Activar validación de certificados** para activar la validación de certificados. Si esta opción está activada, iDRAC6 usa el certificado de CA para validar el certificado del servidor LDAP durante el enlace del nivel de conexión segura (SSL); si está desactivada, iDRAC6 omite el paso de validación de certificados del enlace de SSL. Es posible desactivar la validación de certificados durante las pruebas o si el administrador del sistema decide confiar en los controladores de dominio en el límite de seguridad sin validar sus certificados de SSL.

PRECAUCIÓN: Asegúrese de que la opción CN = abrir LDAP FQDN esté configurada (por ejemplo: CN= openldap.lab) en el campo de asunto del certificado del servidor LDAP, durante la generación del certificado. El campo CN en el certificado del servidor debe estar configurado de tal forma que coincida con el campo de la dirección del servidor LDAP en iDRAC6 para que funcione la validación de certificados.

6. En **Cargar un certificado de CA de Active Directory**, escriba la ruta de acceso al archivo del certificado o examine el equipo para encontrarlo.

   NOTA: Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

7. Haga clic en **Cargar**.

   Se cargará el certificado de CA raíz que firma todos los certificados del servidor SSL de los controladores de dominio.

8. Haga clic en **Siguiente** para ir a la página **Paso 2 de 3 de Configuración y administración del LDAP genérico**. Use esta página para configurar la información de ubicación de los servidores de LDAP genérico y las cuentas de los usuarios.

   NOTA: En esta versión, no se admite la función de autenticación de dos factores (TFA) con tarjeta inteligente ni la función de inicio de sesión único (SSO) para el servicio de directorio de LDAP genérico.

9. Seleccione la opción **Activar LDAP genérico.**

   NOTA: En esta versión no se admite el grupo anidado. El firmware busca al miembro directo del grupo para que coincida con el DN del usuario. Además, sólo se admite un dominio único. No se admiten dominios cruzados.

10. Seleccione la opción **Usar nombre distinguido para buscar la pertenencia a grupos** para emplear el nombre distinguido (DN) como miembros del grupo. iDRAC6 compara el DN del usuario recuperado del directorio para compararlo con los miembros del grupo. Si esta opción no está seleccionada, el nombre de usuario proporcionado por el usuario se utiliza para compararlo con los miembros del grupo.

11. En el campo **Dirección del servidor LDAP**, escriba el nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP. Para especificar múltiples servidores LDAP redundantes que tienen a disposición el mismo dominio, proporcione la lista de todos los servidores separados por comas. iDRAC6 intenta conectar a cada servidor, uno por uno, hasta que logra una conexión exitosa.

12. Introduzca el puerto usado por el LDAP a través de SSL en el campo **Puerto del servidor LDAP**. El valor predeterminado es 636.

13. En el campo **DN de enlace**, escriba el DN de un usuario utilizado para enlazar al servidor durante la búsqueda del DN del usuario. Si no está especificado, se utiliza un enlace anónimo.

14. Introduzca la **Contraseña de enlace** para usarla junto con el **DN de enlace**. Esta opción es obligatoria si no se admite el enlace anónimo.

15. En el campo **DN de base para buscar**, escriba el DN del subdirectorio donde deben iniciarse todas las búsquedas.

16. En el campo **Atributo de inicio de sesión del usuario**, escriba el atributo del usuario a buscar. El valor predeterminado es UID. Se recomienda que este nombre sea único dentro del DN de base seleccionado, pues de lo contrario será necesario configurar un filtro de búsqueda para garantizar la singularidad del usuario. Si el DN del usuario no puede ser identificado en forma exclusiva por la combinación de búsqueda de atributo y filtro de búsqueda, el inicio de sesión fallará.

17. En el campo **Atributo de pertenencia a grupo**, especifique qué atributo de LDAP debe utilizarse para verificar la pertenencia al grupo. Éste deberá ser un atributo de la clase de grupos. Si no está especificado, iDRAC6 usa los atributos de *miembro* y *miembro único*.

18. En el campo **Filtro de búsqueda**, introduzca un filtro de búsqueda de LDAP válido. Use el filtro si el atributo del usuario no logra identificar de forma exclusiva al usuario dentro del DN de base seleccionado. Si no está especificado, el valor predeterminado es *objectClass*=*, que busca todos los objetos en el árbol. Este filtro de búsqueda adicional configurado por el usuario se aplica únicamente para la búsqueda de DN del usuario y no para la búsqueda de pertenencia de grupo.

19. Haga clic en **Siguiente** para ir a la página **Paso 3a de 3** de **Configuración y administración del LDAP genérico**. Use esta página para configurar los grupos de privilegios utilizados para autorizar a los usuarios. Al activar el LDAP genérico, se usan grupos de funciones para especificar la política de autorización para los usuarios de iDRAC6.

20. En **Grupos de funciones**, haga clic en un **Grupo de funciones**.

    Aparece la página **Paso 3b de 3 de Configuración y administración de LDAP genérico.** Use esta página para configurar cada grupo de funciones empleado para controlar la política de autorizaciones de los usuarios.

21. Escriba el **Nombre distinguido (DN) del grupo** que identifica al grupo de funciones en el servicio de directorio de LDAP genérico que está vinculado con el iDRAC6.

22. En la sección **Privilegios del grupo de funciones**, especifique los privilegios asociados con el grupo seleccionando la opción **Nivel de privilegio del grupo de funciones**. Por ejemplo, si selecciona **Administrador**, se seleccionan todos los privilegios para dicho nivel de permiso.

23. Haga clic en **Aplicar** para guardar la configuración del grupo de funciones.

    El servidor web de iDRAC6 automáticamente lo llevará de regreso a la página **Paso 3a de 3 de Configuración y administración de LDAP genérico** donde aparece la configuración de su grupo de funciones.

24. Configure grupos de funciones adiciones de ser necesario.

25. Haga clic en **Terminar** para volver a la **página** de resumen de **Configuración y administración de LDAP**.

26. Haga clic en **Comprobar configuración** para verificar la configuración del LDAP genérico.

27. Escriba el nombre de usuario y la contraseña de un usuario del directorio seleccionado para comprobar la configuración del LDAP. El formato depende del *Atributo de inicio de sesión del usuario* que se utilice, y el nombre de usuario introducido debe coincidir con el valor del atributo seleccionado.

NOTA: Al comprobar la configuración de LDAP con la opción "Activar validación de certificados" marcada, iDRAC6 requiere la identificación del servidor LDAP a través del nombre de dominio completo (FQDN) y no una dirección IP. Si el servidor LDAP es identificado por una dirección IP, la validación de certificados falla, ya que el iDRAC6 no logra comunicarse con el servidor LDAP.

Visualizará los resultados de la prueba y el registro de la misma. Ha completado la configuración del **servicio de directorio del LDAP genérico**.

Preguntas frecuentes

Problemas de inicio de sesión en Active Directory

Iniciar sesión en el iDRAC6 a través del inicio de sesión único de Active Directory lleva aproximadamente 4 minutos.

Si bien el inicio de sesión único normal de Active Directory generalmente demora menos de 10 segundos, puede demorar unos 4 minutos para iniciar sesión en el iDRAC6 a través del inicio de sesión único de Active Directory si especificó el **servidor DNS preferido** y el **servidor DNS alternativo** en la página **Red** del iDRAC6, y el servidor DNS preferido falló. Hay tiempos de espera de DNS cuando un servidor DNS no funciona. El iDRAC6 posibilita el inicio de sesión a través del servidor DNS alternativo.

Configuré Active Directory para un dominio presente en Active Directory de Windows Server 2008 y definí estas configuraciones. Un dominio secundario o subdominio se encuentra presente para el dominio, el usuario y el grupo están presentes en el mismo dominio secundario, y el usuario es miembro de ese grupo. Ahora bien, si intento iniciar sesión en el iDRAC6 mediante el usuario presente en el dominio secundario, el inicio de sesión único de Active Directory falla.

Esto puede deberse a que el tipo de grupo es incorrecto. Existen dos tipos de grupos en el servidor de Active Directory:

- **Seguridad**: Los grupos de seguridad permiten administrar el acceso de usuarios y equipos a los recursos compartidos y filtrar la configuración de política de grupo
- **Distribución**: Los grupos de distribución tienen la finalidad de usarse sólo como listas de distribución por correo electrónico.

Procure siempre que el tipo de grupo sea **Seguridad**. No es posible usar grupos de distribución para asignar permisos para ningún objeto ni usarlos para filtrar la configuración de política de grupo.

No puedo iniciar sesión en Active Directory, ¿qué debo hacer?

iDRAC6 proporciona una herramienta de diagnóstico en la interfaz web.

1. Inicie sesión como usuario local con privilegios de administrador en la interfaz web.
2. En el árbol del sistema, seleccione **Sistema**→ **Acceso remoto**→ **iDRAC6**→ ficha **Red/Seguridad** → **Servicio de directorio**→ **Microsoft Active Directory**.

   Aparece la pantalla de resumen de **Active Directory**.
3. Desplácese hasta la parte inferior de la pantalla y haga clic en **Probar configuración.**

   Aparece la pantalla **Probar configuración de Active Directory**.
4. Ingrese un nombre de usuario de prueba y su contraseña, 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 persisten los problemas, configure los valores de Active Directory, cambie la configuración de usuario y ejecute la prueba nuevamente hasta que el usuario de prueba apruebe el paso de autorización.

Activé la validación de certificados pero no puedo iniciar sesión en Active Directory. Ejecuté los diagnósticos de la interfaz gráfica de usuario y los resultados de la prueba muestran el siguiente mensaje de error. ¿Cuál puede ser el problema y cómo lo soluciono?

```
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 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 rutinas:SSL3_GET_SERVER_CERTIFICATE:error en la validación de certificados: Verifique que se haya 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 el iDRAC concuerda con el sujeto del certificado del servidor de Active Directory.)
```

Si la validación de certificados está activada, el iDRAC6 utiliza el certificado de la entidad emisora cargado para verificar el certificado del servidor de directorio cuando el iDRAC6 establece la conexión SSL con el servidor de directorio. Los motivos más frecuentes de error en la validación de certificados son:

- La fecha del iDRAC6 no se encuentra dentro del período válido del certificado del servidor o del certificado de CA. Verifique la hora del iDRAC6 y el período válido del 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 el iDRAC6 con Active Directory?

Primero, diagnostique el problema con la función Probar configuración. 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 tiene una cuenta de usuario del iDRAC6 local, inicie sesión en el iDRAC6 con las credenciales locales.
   a. Asegúrese de que la casilla **Active Directory activado** esté seleccionada en la página **Paso 2 de 4 Configuración y administración de Active Directory**.
   b. Si activó la validación de certificados, asegúrese de haber cargado el certificado raíz de CA correcto de Active Directory en el iDRAC6. El certificado aparece en el área **Certificado actual de CA de Active Directory**. Asegúrese de que la hora del iDRAC6 se encuentre dentro del período de vigencia del certificado de entidad emisora.
   c. Si está utilizando el esquema extendido, asegúrese de que **Nombre del iDRAC6** y **Nombre de dominio del iDRAC6** coincidan con la configuración del entorno de Active Directory.

      Si está utilizando el esquema estándar, asegúrese de que **Nombre de grupo** y **Dominio del grupo** coincidan con la configuración de Active Directory.
   d. Diríjase a la pantalla **Red**. Seleccione **Sistema→ Acceso remoto→ iDRAC6→ Red/Seguridad→ Red**. Compruebe que la configuración del DNS sea correcta.
   e. Verifique los certificados de controlador de dominio SSL para asegurarse de que la hora del iDRAC6 esté 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 certificados si prefiere confiar en este controlador de dominio sin validación de certificados durante el protocolo de enlace SSL.

¿Por qué el iDRAC6 activa la validación de certificados de manera predeterminada?

El iDRAC6 aplica fuertes medidas de seguridad para asegurar la identidad del controlador de dominio al que se conecta el 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 validación de certificado, puede desactivarla por medio de la interfaz gráfica del usuario o la interfaz de línea de comandos.

Esquema extendido y esquema estándar

Estoy usando un esquema extendido 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 extendido, no puede configurar direcciones de catálogo global, ya que no se usan con éste.

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 el 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

¿El iDRAC6 siempre usa LDAP a través de SSL?

Sí. Todo el transporte se realiza mediante el puerto seguro 636 ó 3269.

Durante la *prueba de la configuración*, el iDRAC6 efectúa una CONEXIÓN A LDAP sólo para ayudar a aislar el problema pero no se vincula a LDAP con una conexión insegura.

¿Admite el iDRAC6 el nombre NetBIOS?

No en esta versión.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de la autentificación de tarjeta inteligente

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

El iDRAC6 admite la función de autentificación por medio de dos factores (TFA) al activar el **inicio de sesión mediante tarjeta inteligente**.

Los esquemas tradicionales de autentificación utilizan nombres de usuario y contraseñas para autentificar a los usuarios. Esto proporciona una seguridad mínima.

En cambio, la función TFA brinda mayor seguridad porque los usuarios deben proporcionar dos factores de autentificación, el que poseen y el que conocen. El factor que se posee es la tarjeta inteligente, un dispositivo físico, y el factor que se conoce es un código secreto, como una contraseña o PIN.

La autentificación de dos factores requiere que los usuarios verifiquen su identidad cuando proporcionan *ambos* factores.

Configuración del inicio de sesión mediante tarjeta inteligente en el iDRAC6

Para activar la función de inicio de sesión mediante tarjeta inteligente del iDRAC6 desde la interfaz web:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Aparece la pantalla **Paso 1 de 4 de Configuración y administración de Active Directory**.
4. Para validar el certificado SSL de los servidores Active Directory, seleccione la casilla **Validación de certificados activada** en **Configuración de certificados**. Si no desea validar el certificado SSL de los servidores Active Directory, vaya directamente a paso 6.
5. En **Cargar 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.** 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 para el certificado de CA de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.
6. Haga clic en Siguiente. Aparece la pantalla **Paso 2 de 4 Configuración y administración de Active Directory**.
7. Seleccione la casilla **Active Directory activado**.
8. Seleccione **Activar inicio de sesión mediante tarjeta inteligente** para activar el inicio de sesión mediante tarjeta inteligente. Se le pedirá el inicio de sesión mediante tarjeta inteligente durante cualquier intento subsiguiente de inicio de sesión mediante la interfaz gráfica de usuario.
9. Agregue el **nombre de dominio del usuario** e introduzca la dirección IP de la dirección de servidor del controlador de dominio. Seleccione **Siguiente**.
10. Seleccione **Configuración del esquema estándar** en la página **Paso 3 de 4 Configuración y administración de Active Directory**. Seleccione **Siguiente**.
11. En la página **Paso 4a de 4 Active Directory**, introduzca la dirección IP del **Servidor de catálogo global**. Agregue la información de grupo de funciones del cual es miembro su usuario válido de Active Directory seleccionando uno de los grupos de funciones (página P**aso 4B de 4 Configurar grupo de funciones**). Introduzca el **nombre del grupo**, el **dominio del grupo** y los **privilegios del grupo de funciones**. Seleccione **Aceptar** y luego **Terminar**. Después de seleccionar **Listo,** desplácese hasta la parte inferior de la página **Active Directory** y seleccione **Carga del archivo keytab de Kerberos**.
12. Cargue un archivo keytab de Kerberos que sea válido. Asegúrese de que las horas del servidor de Active Directory y del iDRAC6 estén sincronizadas. Antes de cargar el archivo keytab, verifique que la hora y la zona horaria sean las correctas. Para obtener más información sobre cómo crear un archivo keytab, consulte "Activación de la autentificación con Kerberos".

Deseleccione la opción **Activar inicio de sesión mediante tarjeta inteligente** para desactivar la función de inicio de sesión mediante tarjeta inteligente con TFA. La próxima vez que inicie sesión en la interfaz gráfica de usuario del iDRAC6, se le pedirá un nombre de usuario y una contraseña local o de Microsoft® Active Directory®, lo cual sucede como solicitud de inicio de sesión predeterminada de la interfaz web.

Inicio de sesión en el iDRAC6 mediante la autentificación con tarjeta inteligente de Active Directory

NOTA: De acuerdo con la configuración del explorador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para lector de tarjeta inteligente cuando utiliza esta función por primera vez.

1. Inicie sesión en el iDRAC6 usando https.

https://<*dirección IP*>

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

https://<*dirección IP*>:<*número de puerto*>

donde *dirección IP* es la dirección IP del iDRAC6 y *número de puerto* corresponde al número de puerto HTTPS.

La página de inicio de sesión del iDRAC6 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente.
3. Introduzca el PIN y haga clic en **Iniciar sesión**.

   De esta forma habrá iniciado sesión en el iDRAC6 con sus credenciales de la forma en que están definidas en Active Directory.

   NOTA: Para mantener la sesión activa, no es necesario que la tarjeta inteligente permanezca en el lector.

Solución de problemas de inicio de sesión con la tarjeta inteligente en el iDRAC6

Utilice los siguientes consejos y sugerencias como ayuda para depurar una tarjeta inteligente que no permite el acceso:

Toma casi 4 minutos iniciar sesión en el iDRAC6 a través del inicio de sesión mediante tarjeta inteligente de Active Directory.

El inicio de sesión normal mediante tarjeta inteligente de Active Directory demora menos de 10 segundos, pero puede tardar casi 4 minutos para iniciar sesión en el iDRAC6 mediante tarjeta inteligente de Active Directory si especificó el **servidor DNS preferido** y el **servidor DNS alternativo** en la página **Red** del iDRAC6, pero falló el servidor DNS preferido. Hay tiempos de espera de DNS cuando un servidor DNS no funciona. El iDRAC6 posibilita el inicio de sesión a través del servidor DNS alternativo.

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes

Compruebe que la tarjeta inteligente sea compatible con el sistema operativo Microsoft Windows®. Windows admite una cantidad limitada de proveedores de servicios criptográficos (CSP) de tarjetas inteligentes.

Consejo: Como verificación general para determinar si los CSP de tarjetas inteligentes están presentes en un cliente particular, inserte la tarjeta inteligente en el lector en la pantalla de inicio de sesión (Ctrl-Alt-Supr) de Windows y revise si Windows detecta esa tarjeta y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente

Revise si la tarjeta inteligente se bloqueó debido a que se hicieron demasiados intentos con PIN incorrectos. En tales casos, el emisor de la tarjeta inteligente en la organización podrá ayudarle a obtener una nueva tarjeta inteligente.

No se puede iniciar sesión en el iDRAC6 como usuario de Active Directory

- Si no puede iniciar sesión en el iDRAC6 como usuario de Active Directory, trate de hacerlo sin activar el inicio de sesión mediante tarjeta inteligente. Puede desactivar el inicio de sesión mediante tarjeta inteligente a través de RACADM por medio del siguiente comando:

  ```
  racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0
  ```

- Para plataformas Windows de 64 bits, el complemento de autentificación del iDRAC6 no se instalará correctamente si se encuentra instalada una versión de 64 bits del "paquete redistribuible de Microsoft Visual C++ 2005". Debe instalar la versión de 32 bits del paquete redistribuible de Microsoft Visual C++ 2005 para que el complemento se instale y se ejecute correctamente.
- Si recibe el siguiente mensaje de error "Not able to load the Smart Card Plug-in. Please check your IE settings or you may have insufficient privileges to use the Smart Card Plug-in (No es posible cargar el complemento de tarjeta inteligente. Verifique la configuración de IE o podría tener privilegios insuficientes para usar el complemento de tarjeta inteligente)", instale el paquete redistribuible Microsoft Visual C++ 2005. Este archivo está disponible en el sitio web de Microsoft en **www.microsoft.com**. Se han probado dos versiones distribuidas del paquete redistribuible de C++, las cuales permiten que se cargue el complemento de tarjeta inteligente de Dell:

Tabla 7-1. Versiones distribuidas del paquete redistribuible de C++

Nombre de archivo del paquete redistribuible	Versión	Fecha de la versión	Tamaño	Descripción
vcredist_x86.exe	6.0.2900.2180	21 de marzo de 2006	2.56 MB	Redistribuible 2005 de Microsoft
vcredist_x86.exe	9.0.21022.8	7 de noviembre de 2007	1.73 MB	Redistribuible 2008 de Microsoft

- Asegúrese de que la hora del iDRAC6 y la del controlador de dominio en el servidor del controlador de dominio no presenten más de 5 minutos de diferencia para que funcione la autentificación con Kerberos. Consulte la **hora del iDRAC6** en la página **Sistema→ Acceso remoto→ iDRAC6→ Propiedades→ Información de acceso remoto**, y la hora del controlador de dominio haciendo clic con el botón derecho del mouse en la hora en el

extremo inferior derecho de la pantalla. La diferencia de zona horaria se muestra en la pantalla emergente. Para la hora estándar de la zona central (CST) de los EE. UU., la diferencia es -6. Use el siguiente comando RACADM de diferencia de zona horaria para sincronizar la hora del iDRAC6 (a través de RACADM remoto o Telnet/SSH): `racadm config -g cfgRacTuning –o cfgRacTuneTimeZoneOffset <valor de diferencia en minutos>`. Por ejemplo, si la hora del sistema es GMT -6 (CST de los EE. UU.) y la hora es 2 p.m., establezca la hora del iDRAC6 en la hora GMT 18:00, lo cual requeriría que introduzca "360" en el comando anterior para especificar la diferencia. También puede usar `cfgRacTuneDaylightoffset` para activar la variación de horario de verano. Esto permite evitar el cambio de la hora las dos veces por año en que se realizan los ajustes de horario de verano, o simplemente hágalo especificando una diferencia de "300" en el ejemplo anterior.

Regresar a la página de contenido

Regresar a la página de contenido

Activación de la autentificación con Kerberos

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Kerberos es un protocolo de autentificación de red que permite que los sistemas se comuniquen de forma segura a través de una red sin protección. Para ello, los sistemas deben demostrar su autenticidad. Para mantener los más altos estándares de cumplimiento de autentificación, el iDRAC6 ahora admite la autentificación de Active Directory® con Kerberos para permitir el inicio de sesión único (SSO) y con tarjeta inteligente en Active Directory.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® y Windows Server 2008 utilizan Kerberos como método de autentificación predeterminado.

El iDRAC6 utiliza Kerberos para admitir dos tipos de mecanismos de autentificación: El inicio de sesión único y con tarjeta inteligente en Active Directory. Para el inicio de sesión único, el iDRAC6 emplea las credenciales de usuario almacenadas en caché en el sistema operativo al iniciar sesión mediante una cuenta válida de Active Directory.

Para el inicio de sesión con tarjeta inteligente de Active Directory, el iDRAC6 utiliza la autentificación de dos factores (TFA) con tarjeta inteligente a modo de credenciales para permitir el inicio de sesión en Active Directory.

La autentificación de Kerberos en el iDRAC6 fallará si la hora del iDRAC6 difiere de la hora del controlador de dominio. Se permite una diferencia máxima de 5 minutos. Para permitir una autentificación correcta, sincronice la hora del servidor con la hora del controlador de dominio y después **restablezca** el iDRAC6.

También puede utilizar el siguiente comando de diferencia de zona horaria de RACADM para sincronizar la hora:

```
racadm config -g cfgRacTuning -o

cfgRacTuneTimeZoneOffset <valor de diferencia>
```

Prerrequisitos para el inicio de sesión único y la autentificación de Active Directory mediante tarjeta inteligente

- Configure el iDRAC6 para el inicio de sesión de Active Directory.
- Registre el iDRAC6 como equipo en el dominio raíz de Active Directory.
  a. Haga clic en **Sistema→ Acceso remoto→ iDRAC6→ Red / Seguridad→** subficha **Red**.
  b. Indique una dirección IP de **servidor DNS alternativo / preferido** que sea válida. Este valor señala la dirección IP del servidor DNS que forma parte del dominio raíz, que autentifica las cuentas de Active Directory de los usuarios.
  c. Seleccione **Registrar el iDRAC6 en el DNS**.
  d. Brinde un **nombre de dominio DNS** válido.
  e. Verifique que la configuración de DNS de la red coincida con la información de DNS de Active Directory.

  Consulte la ayuda en línea del iDRAC6 para obtener más información.

Para permitir el uso de los dos nuevos mecanismos de autentificación, el iDRAC6 admite la configuración para activarse como servicio "kerberizado" en una red Windows con Kerberos. La configuración de Kerberos en el iDRAC6 requiere los mismos pasos que la configuración de un servicio Kerberos externo a Windows Server como principal función de seguridad en Windows Server Active Directory.

La herramienta **ktpass** de Microsoft (proporcionada por Microsoft como parte del CD/DVD de instalación del servidor) se utiliza para crear el enlace del nombre principal de servicio (SPN) con una cuenta de usuario y exportar la información de confianza a un archivo *keytab* de Kerberos de tipo MIT, lo que permite establecer una relación de confianza entre un usuario o sistema externo y el centro de distribución de claves (KDC). El archivo keytab contienen una clave criptográfica que se usa para cifrar la información entre el servidor y el KDC. La herramienta ktpass permite el uso de servicios basados en UNIX que admiten la autentificación Kerberos para ejecutar las funciones de interoperabilidad proporcionadas por un servicio Kerberos KDC de Windows Server.

El archivo keytab que se obtiene de la utilidad ktpass está disponible para el iDRAC6 como archivo para cargar y está activado para actuar como un servicio kerberizado en la red.

Como el iDRAC6 es un dispositivo con un sistema operativo que no es Windows, ejecute la utilidad **ktpass** (que es parte de Microsoft Windows) en el controlador de dominio (servidor Active Directory) donde desea asignar el iDRAC6 a una cuenta de usuario de Active Directory.

Por ejemplo, utilice el comando **ktpass** a continuación para crear el archivo keytab de Kerberos:

```
C:\> ktpass.exe -princ HTTP/idracname.domainname.com@DOMAINNAME.COM -mapuser DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL -pass <contraseña> +DesOnly -out c:\krbkeytab
```

NOTA: Si tiene algún problema con el usuario de iDRAC6 para quien se crea el archivo keytab, cree un nuevo usuario y un nuevo archivo keytab. Si se ejecuta nuevamente el mismo archivo keytab que se creó inicialmente, no se configurará correctamente.

Luego de que el comando anterior se ejecute correctamente, ejecute el siguiente comando:

```
C:\>setspn -a HTTP/nombre_de_idrac.nombre_de_dominio.com nombre_de_usuario
```

El tipo de cifrado admitido por el iDRAC6 para la autentificación con Kerberos es DES-CBC-MD5. El tipo principal es KRB5_NT_PRINCIPAL. La siguiente propiedad de la cuenta de usuario a la que está asignado el nombre principal de servicio deberá estar **activada**:

- Usar tipos de cifrado DES para esta cuenta

NOTA: Debe crear una cuenta de usuario de Active Directory para usar con la opción -mapuser del comando **ktpass**. Además, debe tener el mismo nombre que el nombre del iDRAC6 en el DNS para el que cargará el archivo keytab generado.

NOTA: Se recomienda usar la utilidad **ktpass** más reciente para crear el archivo keytab. Además, al generar el archivo keytab, use letras *minúsculas* para el **nombre_de_idrac** y el **nombre principal de servicio**.

Este procedimiento generará un archivo keytab que deberá cargar en el iDRAC6.

NOTA: Este archivo contiene una clave de cifrado y debe mantenerse guardado de manera segura.

Para obtener más información sobre la utilidad **ktpass**, visite el sitio web de Microsoft: **http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

- La hora del iDRAC6 debe sincronizarse con el controlador de dominio de Active Directory.

Configuración del iDRAC6 para el inicio de sesión único y la autentificación de Active Directory mediante tarjeta inteligente

Cargue en el iDRAC6 el archivo keytab obtenido del dominio raíz de Active Directory:

1. Haga clic en **Sistema→ Acceso remoto→ iDRAC6→ Red/Seguridad→ Servicio de directorios→ Microsoft Active Directory**
2. En la parte inferior de la página resumen de **Active Directory**, haga clic en **Cargar keytab de kerberos**.
3. En la página **Cargar keytab de Kerberos**, seleccione el archivo keytab que desea cargar y haga clic en **Aplicar**.

También puede cargar el archivo en el iDRAC6 mediante comandos racadm de la interfaz de línea de comandos. El siguiente comando permite cargar el archivo keytab en iDRAC6:

```
racadm krbkeytabupload -f <nombre_de_archivo>
```

donde <*nombre_de_archivo*> es el nombre del archivo keytab.

Configuración de usuarios de Active Directory para el inicio de sesión único

Antes de usar la función de inicio de sesión único de Active Directory, asegúrese de que el iDRAC6 ya está configurado para el inicio de sesión de Active Directory y de que la cuenta de usuario de dominio que se utilizará para iniciar sesión en el sistema está activada para el inicio de sesión en Active Directory del iDRAC6.

Asimismo, verifique que la configuración de inicio de sesión de Active Directory está activada. El iDRAC6 también debe estar activado para representar un servicio kerberizado. Para ello es necesario cargar en el iDRAC6 un archivo *keytab* válido obtenido del dominio raíz de Active Directory.

Inicio de sesión en el iDRAC6 con la función de inicio de sesión único para usuarios de Active Directory

NOTA: Para iniciar sesión en el iDRAC6, asegúrese de contar con los más recientes componentes en tiempo de ejecución de las bibliotecas Microsoft Visual C++ 2005. Para obtener más información, consulte el sitio web de Microsoft.

1. Inicie sesión en el sistema por medio de una cuenta de Active Directory válida.
2. Escriba el nombre del iDRAC6 en la barra de dirección del explorador con el siguiente formato: **https://nombre_de_idrac.nombre_de_dominio.com** (por ejemplo, **https://prueba-idrac.dominio.com**).

   NOTA: De acuerdo con la configuración del explorador, el sistema puede solicitarle que descargue e instale el complemento para inicio de sesión único cuando utiliza esta función por primera vez.

   NOTA: Para SSO, si utiliza Internet Explorer, diríjase a **Herramientas→ Opciones de Internet→** ficha **Seguridad→ Intranet local→** haga clic en **Sitios→** haga clic en **Avanzado** y luego agregue la anotación ***.dominio.com** en la zona. Si usa Firefox, escriba **about:config** y luego agregue **dominio.com** para las propiedades **network.negotiate-auth.delegation-uris** y **network.negotiate-auth.trusted-uris**.

   Usted estará conectado al iDRAC6 con los privilegios adecuados de Microsoft Active Directory si:

   - Es usuario de Microsoft Active Directory

- Está configurado en el iDRAC6 para el inicio de sesión de Active Directory
- El iDRAC6 está activado para la autentificación de Active Directory con Kerberos

---

Configuración de usuarios de Active Directory para inicio de sesión con tarjeta inteligente

Antes de usar la función de inicio de sesión con tarjeta inteligente de Active Directory, asegúrese de que el iDRAC6 ya esté configurado para el inicio de sesión de Active Directory y de que la cuenta de usuario para la que se emitió la tarjeta inteligente está activada para el inicio de sesión en Active Directory del iDRAC6.

Asimismo, verifique que la configuración de inicio de sesión de Active Directory está activada. El iDRAC6 también debe estar activado para representar un servicio kerberizado. Para ello es necesario cargar en el iDRAC6 un archivo *keytab* válido obtenido del dominio raíz de Active Directory.

NOTA: Las funciones de autentificación de dos factores (TFA) con tarjeta inteligente e inicio de sesión único (SSO) no pueden utilizarse si Active Directory está configurado para el esquema ampliado. Además, la TFA con tarjeta inteligente y el inicio de sesión único se admiten en sistemas operativos Microsoft Windows con Internet Explorer®. La TFA con tarjeta inteligente **no** se admite en exploradores Firefox, mientras que el inicio de sesión único en iDRAC6 es compatible con los exploradores Firefox.

PRECAUCIÓN: Para iniciar sesión en el iDRAC6, asegúrese de contar con los más recientes componentes en tiempo de ejecución de las bibliotecas Microsoft Visual C++ 2005 instaladas (biblioteca C++ de 32 bits). De lo contrario, el complemento de tarjeta inteligente no se cargará y usted no podrá iniciar sesión en el iDRAC6. Para obtener más información, visite el sitio web de Microsoft (www.microsoft.com).

Usted estará conectado al iDRAC6 con los privilegios adecuados de Microsoft Active Directory si:

- Es usuario de Microsoft Active Directory
- Está configurado en el iDRAC6 para el inicio de sesión de Active Directory
- El iDRAC6 está activado para la autentificación de Active Directory con Kerberos
- Ha introducido el PIN correcto para la tarjeta inteligente relacionada con el usuario de Active Directory que intenta iniciar sesión

---

Situaciones de inicio de sesión en el iDRAC6 con TFA y SSO

Cuando inicia sesión en el iDRAC6 desde la interfaz gráfica de usuario del CMC, iDRAC6 muestra las siguientes opciones en pantalla de inicio de sesión para diversas combinaciones de activación de TFA y SSO, con versiones diferentes de iDRAC/iDRAC6 y CMC:

- **CMC v2.1 o posterior con TFA activada e iDRAC6 v2.1 o posterior con TFA activada:** Petición de inicio de sesión de iDRAC6 con ingreso de PIN.
- **CMC v2.1 o posterior con TFA activada e iDRAC6 v2.1 o posterior con TFA desactivada y SSO desactivado:** Petición de inicio de sesión de iDRAC6 con nombre de usuario, dominio y contraseña.
- **CMC v2.1 o posterior con TFA activada e iDRAC6 v2.1 o posterior con TFA desactivada y SSO activado:** El iDRAC6 inicia sesión automáticamente con SSO.
- **CMC v2.1 o posterior con TFA activada e iDRAC6 v2.0:** Petición de inicio de sesión de iDRAC6 con nombre de usuario, dominio y contraseña.
- **CMC v2.1 o posterior con TFA activada e iDRAC 1.*x*:** Petición de inicio de sesión de iDRAC6 con nombre de usuario, dominio y contraseña.
- **CMC v2.0 o anterior e iDRAC6 2.1 o posterior con TFA activada:** Petición de inicio de sesión de iDRAC6 con ingreso de PIN.
- **CMC v2.1 o posterior con TFA desactivada e iDRAC6 v2.1 con TFA activada y SSO desactivada:** Petición de ingreso de PIN de iDRAC6.
- **CMC v2.1 o posterior con TFA desactivada e iDRAC6 v2.1 o posterior con TFA desactivada y SSO activada:** El iDRAC6 inicia sesión con SSO.

Regresar a la página de contenido

Regresar a la página de contenido

Visualización de la configuración y la condición del servidor administrado

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

---

Resumen del sistema

La página **Resumen del sistema** le permite visualizar la condición del sistema y otra información básica del iDRAC6 y le proporciona vínculos de acceso a las páginas sobre la condición e información del sistema. Además, desde esta página puede iniciar rápidamente tareas comunes y ver los sucesos recientes registrados en Registro de sucesos del sistema (SEL).

Para acceder a la página **Resumen del sistema**, haga clic en **Sistema**→ ficha **Propiedades** → **Resumen del sistema.** Consulte la Ayuda en línea del iDRAC6 para obtener información detallada sobre cada sección de la página **Resumen del sistema**.

Detalles del sistema

La página **Resumen del sistema** muestra información sobre los siguientes componentes del sistema:

- Gabinete del sistema principal
- Integrated Dell Remote Access Controller 6: Enterprise

Gabinete del sistema principal

Información del sistema

Esta sección de la interfaz web del iDRAC6 brinda la siguiente información básica sobre el 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.
- 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.

NOTA: El campo **Nombre del sistema operativo** se completa sólo si Dell OpenManage™ Server Administrator está instalado en el sistema administrado. Representan una excepción los nombres de sistemas operativos VMware®, que se muestran aun si Server Administrator no está instalado en el sistema 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 de modelo de la tarjeta de almacenamiento instalada, por ejemplo, SAS6/iR

Recuperación automática

Esta sección de la interfaz web del iDRAC6 detalla el modo de operación actual de la función de recuperación automática 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 Sin **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: Muestra la fecha y hora actuales (del momento de la última actualización de la página) del iDRAC6.
- Versión del firmware: Muestra la versión actual del firmware del iDRAC6 instalada en el sistema administrado.
- Versión de CPLD: Muestra la versión del dispositivo lógico programable complejo (CPLD) de la placa base.
- Actualización del firmware: Muestra la fecha y hora de la última actualización exitosa del firmware del iDRAC6.
- Dirección MAC: Muestra la dirección MAC asociada con el controlador de interfaz de red de LOM (LAN de la placa base) del iDRAC6.

Configuración de IPv4

- Activado: Muestra si está activada o desactivada la compatibilidad con el protocolo IPv4.

  NOTA: La opción del protocolo IPv4 está activada de manera predeterminada.

- DHCP activado: Activado si el iDRAC6 está configurado para tomar su dirección IP e información asociada de un servidor DHCP.
- Dirección IP: Muestra la dirección IP asociada con el iDRAC6 (no el servidor administrado).
- Máscara de subred: Muestra la máscara de subred TCP/IP configurada para el iDRAC6.
- Puerta de enlace: Muestra la dirección IP de la puerta de enlace de red configurada para el iDRAC6.
- Usar DHCP para obtener direcciones del servidor DNS: Muestra si se usa el DHCP para obtener direcciones del servidor DNS.
- Servidor DNS preferido: Muestra el servidor DNS primario actualmente activo.
- Servidor DNS alternativo: Muestra la dirección del servidor DNS alternativo.

configuración de IPv6

- Activado: Muestra si está activada o desactivada la compatibilidad con el protocolo IPv6.
- Configuración automática activada: Muestra si la configuración automática está activada o desactivada.
- Dirección local del vínculo: Muestra la dirección IPv6 para la NIC del iDRAC6.
- Dirección de IPv6 1-16: Muestra hasta 16 direcciones IPv6 (Dirección IPv6 1 a dirección IPv6 16) para la NIC del iDRAC6.
- Puerta de enlace: Muestra la dirección IP de la puerta de enlace de red configurada para el iDRAC6.
- Usar DHCPv6 para obtener direcciones del servidor DNS: Muestra si se usa el DHCP para obtener direcciones del servidor DNS.
- Servidor DNS preferido: Muestra el servidor DNS primario actualmente activo.
- Servidor DNS alternativo: Muestra la dirección del servidor DNS alternativo.

NOTA: Esta información también está disponible en **iDRAC6→ Propiedades→ Información de acceso remoto**.

Dirección MAC de la NIC incorporada

- NIC 1: Muestra las direcciones de control de acceso al medio (MAC) del controlador de interfaces de red (NIC) incorporado 1. Las direcciones MAC identifican de forma particular cada nodo en una red en la capa de control de acceso al medio. El NIC de la interfaz de sistema para equipos pequeños (iSCSI) de Internet es un controlador de interfaces de red con la pila de iSCSI ejecutándose en el equipo host. Los NIC de Ethernet admiten el estándar de Ethernet cableado y enchufado en el bus del sistema del servidor.
- NIC 2: Muestra las direcciones MAC del NIC 2 incorporado que lo identifica de forma particular en la red.
- NIC 3: Muestra las direcciones MAC del NIC 3 incorporado que lo identifica de forma particular en la red. Es probable que las direcciones MAC del NIC 3 incorporado no aparezcan en todos los sistemas.
- NIC 4: Muestra las direcciones MAC del NIC 4 incorporado que lo identifica de forma particular en la red. Es probable que las direcciones MAC del NIC 4 incorporado no aparezcan en todos los sistemas.

WWN / MAC

Haga clic en **Sistema**→ ficha **Propiedades**→ **WWN / MAC** para ver la configuración actual de las tarjetas intermedias de E/S instaladas y sus redes Fabric relacionadas. Si la función FlexAddress está activada en el CMC, las direcciones MAC persistentes asignadas globalmente (asignadas por el chasis) reemplazarán a los valores de cableado de cada LOM.

Condición del servidor

Haga clic en la sección **Sistema**→ ficha **Propiedades**→ **Resumen del sistema** → **Condición del servidor** para ver información importante acerca de la condición del iDRAC6 y los componentes supervisados por el iDRAC6. La columna de **Estado** muestra el estado de cada componente. Para obtener una lista de símbolos de estado y su significado, consulte Tabla 20-3. Haga clic en el nombre del componente en la columna **Componente** para obtener información más detallada acerca de éste.

NOTA: La información del componente también puede obtenerse con un clic sobre su nombre en el panel izquierdo de la ventana. Los componentes permanecen visibles en el panel izquierdo independientemente de la ficha/pantalla seleccionada.

iDRAC6

La pantalla **Información de acceso remoto** enumera una serie de detalles importantes acerca del iDRAC6, como el nombre, la revisión del firmware, la actualización del firmware, la hora del iDRAC6, la versión de IPMI, la versión de CPLD, el tipo de servidor y los parámetros de la 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 condición, la revisión del firmware y las direcciones IP de 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 de firmware de Chassis Management Controller* para obtener más información.

NOTA: Al iniciar la interfaz gráfica web del CMC desde el iDRAC6, la búsqueda tendrá el mismo formato de dirección IP. Por ejemplo, si abre la interfaz gráfica web del iDRAC6 con formato de dirección IPv6, la página web del CMC también abrirá una dirección IPv6 válida.

Baterías

La pantalla **Baterías** muestra el estado 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 **Temperaturas** muestra el estado y las lecturas de la sonda de temperatura ambiente integrada. Se muestran los umbrales de temperatura mínima y máxima para estados de *advertencia* y *falla*, junto con la condición actual de la sonda.

NOTA: Según el modelo del servidor, es posible que no se muestren los umbrales de temperatura para los estados de *advertencia* y *falla* y/o la condición de la sonda.

Voltajes

La pantalla **Sondas de voltaje** muestra el estado y las lecturas de estas sondas e informa acerca del estado del riel de voltaje incorporado y los sensores de núcleo de la CPU.

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 (valor promedio en un minuto, medido en vatios de CA) que está usando el servidor de acuerdo con lo informado por el monitor actual de la placa de sistema.
- Amperaje: Muestra el consumo (corriente alterna en amperios) en la unidad de suministro de energía activa.
- Estadísticas de seguimiento de alimentación: Informa la cantidad de energía utilizada por el sistema desde el último restablecimiento de la lectura.
- Estadísticas pico: Informa la cantidad pico de energía utilizada por el sistema desde el último restablecimiento de la lectura.
- Consumo de alimentación: Muestra el consumo de energía mínimo, promedio y máximo, así como las fechas y horas de alimentación máximas y mínimas en el sistema para el minuto, la hora, el día y la semana últimos.
- Mostrar gráfica: Muestra una representación gráfica del consumo de energía para 1 hora, 24 horas, 3 días y 1 semana.

NOTA: La alimentación y el amperaje se miden en corriente alterna.

CPU

La pantalla **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 de la 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.
- Pantalla de 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**→ ficha **Registros**→ **Registro de sucesos del sistema**.

Regresar a la página de contenido

Regresar a la página de contenido

Supervisión y administración de alimentación

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Los sistemas Dell™ PowerEdge™ traen muchas características nuevas y mejoradas de administración de energía. El diseño de toda la plataforma, desde el hardware al firmware, pasando por el software de administración de sistemas, está orientado a la eficacia energética, y a la supervisión y administración de energía.

NOTA: La lógica de administración de energía del iDRAC6 utiliza un dispositivo lógico programable complejo, denominado CPLD por sus siglas en inglés, que se encuentra en el servidor Blade. Las actualizaciones de los dispositivos CPLD están disponibles en el sitio web de asistencia de Dell (**support.dell.com**), en las secciones **Firmware del sistema** o **Placa base**. Se recomienda actualizar el servidor blade con la versión más reciente de firmware de CPLD. La actual versión de firmware de CPLD se muestra en la interfaz gráfica del usuario del iDRAC6.

Los sistemas Dell 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 web del iDRAC6 se puede ver esta información en la pantalla **Supervisión de alimentación**. También se 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 "Supervisión de alimentación".
- **Presupuesto de alimentación:** durante el inicio, un inventario del sistema permite calcular el presupuesto de alimentación de la configuración actual. Consulte "[Presupuesto de alimentación]" para obtener más información.
- **Control de alimentación:** el iDRAC6 permite realizar varias acciones de administración de la energía 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 web del iDRAC6 y la interfaz de línea de comandos (CLI) de RACADM para administrar y configurar los controles de alimentación en el sistema Dell 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 energía mínimo y máximo. Consulte "Ver el presupuesto de alimentación".
- Ver el umbral del presupuesto de alimentación del servidor. Consulte "Umbral de presupuesto de alimentación".
- Ejecutar operaciones de control de alimentación en el servidor (por ejemplo, encendido, apagado, restablecimiento del sistema, ciclo de encendido y apagado ordenado). Consulte "Ejecución de operaciones de control de alimentación en el servidor".

Supervisión de alimentación

El iDRAC6 supervisa el consumo de energía en los servidores Dell PowerEdge en forma continua. El iDRAC6 calcula los siguientes valores de alimentación y proporciona la información a través de su interfaz web o de línea de comandos de RACADM:

- Potencia acumulada del sistema
- Potencia pico y amperaje pico del sistema
- Consumo de energía promedio, mínimo y máximo
- Consumo de energía (también puede verlo en gráficas en la interfaz web)
- Fechas y horas de alimentación máx. y mín.

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,** con la siguiente información:

Supervisión de alimentación

- **Estado**: Una **marca de verificación verde** indica que el estado de la alimentación es normal**, Advertencia** indica que se ha emitido una alerta de advertencia y **Grave** indica que se ha emitido una alerta de falla.
- **Nombre de la sonda**: Indica el nombre del sensor.
- **Lectura**: Indica el vataje informado por la sonda.
- **Umbral de advertencia**: Muestra el consumo de energía aceptable (en vatios y BTU/h) recomendados para el funcionamiento del sistema. El consumo de energía que exceda este valor produce sucesos de advertencia.
- **Umbral de falla**: Muestra el consumo de energía aceptable más alto (en vatios y BTU/h) requerido para el funcionamiento del sistema. El consumo de energía que exceda este valor produce sucesos de falla/críticos.

Amperaje

- **Ubicación**: Muestra el nombre del sensor de la placa del sistema.
- **Lectura**: El consumo actual de corriente alterna, en amperios

Estadísticas de seguimiento de alimentación y estadísticas pico

- **Estadística:**
  - **Potencia 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.
  - **Potencia pico del sistema** especifica el valor pico del sistema, en vatios de corriente alterna.
  - **Amperaje pico del sistema** especifica el amperaje pico del sistema. El valor pico es el valor más alto registrado entre la **hora inicial de medición** y ahora. La hora pico fue el momento en que ocurrió el valor pico. Haga clic en **Restablecer** al final de la fila de la tabla para volver a establecer el valor instantáneo actual (el cual no será 0 si el servidor está en funcionamiento). Al seleccionar el restablecimiento, también se restablecerá la hora inicial de medición y se fijará la hora actual.
  - **La Hora inicial 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 **Potencia acumulada del sistema**, **Amperaje pico del sistema** y **Potencia pico del sistema**, los valores pico, al restablecerse, mostrarán inmediatamente el valor instantáneo actual.
  - **La Hora actual de medición** para la **Potencia 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 **Potencia pico del sistema**, los campos de **Hora pico** muestran la hora en que tuvieron lugar dichos picos.
  - **Lectura**: el valor de la estadística correspondiente (**Potencia acumulada del sistema**, **Potencia pico del sistema** y **Amperaje pico del sistema**) desde que se inició el contador.

NOTA: Se mantienen estadísticas de seguimiento de alimentación luego de todos los restablecimientos del sistema. De este modo se refleja toda la actividad en el intervalo entre la hora de inicio y la actual. Los valores de alimentación que se muestran en la tabla de consumo de energía son promedios acumulados en el intervalo de tiempo respectivo (minuto, hora, día y semana últimos). 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 máximos de alimentación (máximos en vatios en comparación con consumo máximo de energía) pueden ser distintos.

Consumo de energía

- **Consumo de energía promedio**: Promedio sobre minuto, hora, día y semana anteriores.
- **Consumo de energía máximo y Consumo de energía mínimo:** El consumo de energía 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 energía 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]

La pantalla **Presupuesto de alimentación** muestra los límites de los umbrales de alimentación, los cuales cubren el rango de consumos de energía en corriente alterna que presenta al centro de datos un sistema con una gran carga de trabajo.

Antes de que un servidor se encienda, el iDRAC6 le proporciona al CMC los requisitos de envolvente de potencia. El iDRAC6 puede solicitar una envolvente de potencia inferior una vez encendido el servidor, de acuerdo con la energía real consumida por éste. Si el consumo de energía aumenta con el tiempo y el consumo del servidor se acerca a su asignación máxima, el iDRAC6 puede requerir un aumento del consumo de energía máximo potencial, lo que incrementa la envolvente de potencia. El iDRAC6 sólo aumenta el requisito de consumo de energía máximo potencial para el CMC y no requiere un mínimo de alimentación potencial inferior si el consumo disminuye.

El CMC recupera toda energía sin utilizar de los servidores de menor prioridad, y luego asigna la energía recuperada a un servidor o módulo de infraestructura de mayor prioridad.

Ver el presupuesto de alimentación

El servidor proporciona una descripción general del estado del presupuesto de alimentación del subsistema de alimentación en la pantalla **Presupuesto de alimentación**.

Por medio de la interfaz web

NOTA: Para realizar acciones de administración de energía, se debe contar con privilegios de **Administrador**.

1. Inicie sesión en la interfaz web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema.**
3. Haga clic en la ficha **Administración de la alimentación** y luego en **Presupuesto de alimentación**.

   Aparecerá la pantalla **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 corriente alterna que presenta al centro de datos un sistema con umbrales con una gran carga de trabajo.

- **El consumo de energía potencial mínimo** representa el valor más bajo del umbral de presupuesto de alimentación.
- **El consumo de energía potencial máximo** representa el valor más alto del umbral de presupuesto de alimentación. Este valor es también el consumo de energía máximo absoluto de la configuración actual del sistema.

Uso de RACADM

En un servidor 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".

Umbral de 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 energía cerca del umbral determinado.

El consumo de energía real puede ser menor en cargas de trabajo más livianas y puede exceder el umbral de forma momentánea hasta completar los ajustes de rendimiento.

Por medio de la interfaz web

1. Inicie sesión en la interfaz web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema.**
3. Haga clic en la ficha **Administración de la alimentación** y luego en **Presupuesto de alimentación**.

   Aparecerá la pantalla **Presupuesto de alimentación**.
4. Haga clic en **Umbral del presupuesto de alimentación**.

NOTA: El umbral del presupuesto de alimentación es de sólo lectura. No es posible activarlo ni configurarlo en el iDRAC6.

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** muestran el límite en vatios de corriente alterna y BTU/h, respectivamente.
- **Umbral en porcentaje (del máximo)** muestra el porcentaje del rango de límites de alimentación.

Uso de RACADM

En un servidor administrado, abra una interfaz de línea de comandos y escriba:

Para ver los datos del umbral del presupuesto de alimentación de RACADM local, introduzca el siguiente texto en la petición de comandos:

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapWatts
```

Informa <*valor límite de alimentación en vatios de CA*>

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapBTUhr
```

Informa <*valor límite de alimentación en BTU/h*>

```
racadm getconfig -g cfgServerPower -o cfgServerPowerCapPercent
```

Informa <*valor límite de alimentación en %*>

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 de manera remota: Encendido, apagado, 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**.

El iDRAC6 le permite realizar de manera 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 **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 interrumpir la operación del 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. Esta acción se desactivará si el sistema ya está apagado.
   - **Apagado ordenado:** Intenta cerrar de manera estructurada el sistema operativo y luego apaga el sistema. Para efectuar un 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. Esta acción se desactivará si el sistema ya está apagado.
   - **Restablecer el sistema (reinicio mediante sistema operativo)** reinicia el sistema sin apagarlo. Esta acción se desactivará si el sistema ya está apagado.
   - **Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)** 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

Para realizar acciones de alimentación desde RACADM local, introduzca el siguiente texto en la petición de comando:

```
racadm serveraction <acción>
```

donde <acción> es encendido, apagado, ciclo de encendido, apagado no ordenado, o estado de alimentación.

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

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

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 Blade desde cualquier lugar con acceso a la red. Los beneficios de SOL son los siguientes:

- Acceder de forma remota a los sistemas operativos sin que expire el tiempo.
- Realizar diagnósticos de sistemas host en servicios de administración de emergencia (EMS) o en la consola administrativa especial (SAC) para Windows o un shell de Linux.
- Ver el progreso de un servidor Blade 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 herramienta IPMI)
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:

   - Apagado
   - Encendido sin redirección de consola
   - Encendido con redirección de consola

   Utilice las teclas de flecha para recorrer las opciones.
4. Asegúrese de que la opción **Encendido con redirección de consola** esté activada. Asegúrese de que la opción **Dirección del puerto serie** sea COM1.
5. Verifique que el valor de **Velocidad en baudios a prueba de fallas** sea idéntico a la velocidad en baudios de SOL configurada en el iDRAC6. El valor predeterminado la velocidad en baudios a prueba de fallas y la velocidad en baudios de SOL configurada en el iDRAC6 es 115,2 kbps.
6. Asegúrese de que la opción **Redirección después de inicio** esté activada. Esta opción activa la redirección de SOL del BIOS en los reinicios subsecuentes. El BIOS cuenta con los valores VT100/VT220 y ANSI para **Tipo de terminal remota**.
7. Guarde los cambios y salga.

   El servidor administrado se reinicia.

Configuración de la comunicación en serie en la LAN en la interfaz gráfica para el usuario del iDRAC6

1. Abra la pantalla **Configuración de la comunicación en serie en la LAN** de la siguiente manera: Seleccione **Sistema→ Acceso remoto→ iDRAC6→**

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 9600 bps, 19,2 kbps, 57,6 kbps y 115,2 kbps. El valor predeterminado es 115,2.

4. Seleccione un límite de nivel de privilegios de la comunicación en serie en la LAN.

   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.

5. Haga clic en **Aplicar** si realizó cambios.

Tabla 10-1. 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 **9600 bps**, **19,2 kbps**, **57,6 kbps** ó **115,2 kbps**.
Límite del nivel de privilegios del canal	Seleccione un límite de nivel de privilegios de la comunicación en serie en la LAN.

Tabla 10-2. 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 **Comunicación en serie en la LAN.**
Configuración avanzada	Abre la pantalla **Configuración avanzada de la comunicación en serie en la LAN**.
Aplicar	Aplica los nuevos valores de configuración asignados mientras se visualiza la pantalla **Comunicación en serie en la LAN**.

6. Cambie la configuración en la pantalla **Configuración avanzada de la comunicación en serie en la LAN**, de ser necesario. Se recomienda usar 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 255 caracteres respectivamente.

Tabla 10-3. 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.
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 10-4. 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 **Comunicación en serie en la LAN**.

7. Configure SSH y Telnet para SOL en **Sistema→ Acceso remoto→ iDRAC6→** ficha **Red/Seguridad → Servicios**.

NOTA: Cada servidor Blade admite sólo una sesión SOL activa.

NOTA: El protocolo SSH está activado de manera predeterminada. De manera predeterminada, el protocolo Telnet está desactivado.

8. Haga clic en **Servicios** para abrir la pantalla **Servicios**.

   NOTA: Los programas SSH y Telnet proporcionan acceso a través de un sistema remoto.

9. Haga clic en **Activado** en **SSH** o **Telnet** según sea necesario.

10. 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 expiración de tiempo se establece en 0. El valor predeterminado es **1800 segundos**.

11. Active la interfaz fuera de banda del iDRAC6 (IPMI en la LAN). Para ello, seleccione **Sistema→ Acceso remoto→ iDRAC6→ Red/Seguridad→ Red**.

12. Seleccione la opción **Activar IPMI en la LAN** en la sección **Configuración de IPMI.**

13. 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, 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 iDRAC6. 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/VT220. La consola en serie se envía automáticamente a la consola de Telnet o SSH.

Para iniciar una sesión SOL, conéctese al iDRAC6 a través de SSH/Telnet, lo cual lo lleva a la consola de línea de comandos del iDRAC6. Escriba "**connect**" a continuación del símbolo de dólar.

Consulte "Instalación de clientes Telnet o SSH" para obtener más información sobre cómo usar clientes Telnet y SSH con el iDRAC6.

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 interfaz gráfica 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, de manera 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 obtener más información: **http://ipmitool.sourceforge.net/manpage.html**.

Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6

Los comandos para desconectar una sesión SOL se centran en la utilidad. Puede salir de la utilidad sólo cuando se haya finalizado por completo la sesión SOL.

Para desconectar una sesión SOL, finalice la sesión SOL desde la consola de línea de comandos del iDRAC6.

Cuando esté listo para salir de la redirección de SOL, presione <Entrar>, <Esc> y después <t> (presione las teclas en secuencia, una tras otra). La sesión SOL se cerrará según corresponda. La secuencia de escape también se muestra en la pantalla al momento de conectarse una sesión SOL. Cuando el servidor administrado está **apagado**, la sesión SOL demora más tiempo en establecerse.

NOTA: Si la sesión SOL no se cierra correctamente en la utilidad, no habrá más sesiones disponibles. Para resolver esta situación, es necesario finalizar la consola de línea de comandos en la interfaz gráfica web en **Sistema→ Acceso remoto→ iDRAC6→ 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 valor de expiración de tiempo predeterminado de SSH/Telnet en **Sistema → Acceso remoto→ iDRAC6 → Red / Seguridad → Servicios**.

1. Para conectarse al iDRAC6, introduzca lo siguiente en el símbolo del sistema:

   `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. Introduzca lo siguiente en el símbolo del sistema para iniciar SOL:

   `connect`

   NOTA: Con esto se conectará al puerto serie del servidor administrado. Una vez que se establece una sesión SOL, la consola de línea de comandos del iDRAC6 ya no estará a su disposición. Siga correctamente la secuencia de escape para llegar a la consola de línea de comandos del iDRAC6. Salga de la sesión de SOL por medio de la secuencia de comandos que se describe en "Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6" e inicie una nueva.

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 valor de expiración de tiempo predeterminado de Telnet en **Sistema→ Acceso remoto→ iDRAC6→ Red / Seguridad→ Servicios**.

1. Inicie una ventana de shell.
2. Para conectarse al iDRAC6, ingrese el comando siguiente:

   `telnet <dirección_IP_iDRAC6>`

   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. Introduzca lo siguiente en el símbolo del sistema para iniciar SOL:

   `connect`

4. 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 suéltelas). 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 valor predeterminado de expiración de tiempo de SSH en **Sistema → Acceso remoto→ iDRAC6 → 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. Introduzca lo siguiente en el símbolo del sistema para iniciar SOL:

```
connect
```

NOTA: Con esto se conectará al puerto serie del servidor administrado. Una vez que se establece una sesión SOL, la consola de línea de comandos del iDRAC6 ya no estará a su disposición. Siga correctamente la secuencia de escape para llegar a la consola de línea de comandos del iDRAC6. Salga de la sesión SOL (consulte "Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6" para cerrar una sesión SOL activa).

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. Consulte la *Guía de instalación rápida del software* para obtener información sobre la instalación. 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 valor predeterminado de expiración de tiempo de SOL en **Sistema → Acceso remoto→ iDRAC6 → Red/Seguridad → Servicios**.

1. Localice el archivo **IPMItool.exe** en el directorio correspondiente.

   La ruta de acceso predeterminada en el sistema operativo Windows de 32 bits es **C:\Archivos de programa\Dell\SysMgt\bmc**, y en el sistema operativo Windows de 64 bits es **C:\Archivos de programa (x86)\Dell\SysMgt\bmc**.

2. Asegúrese de que la **Clave de cifrado** contenga sólo ceros en **Sistema→ Acceso remoto→ iDRAC6→ Red/Seguridad→ Red→ Configuración de IPMI**.

3. Ingrese el siguiente comando en el indicador de comandos de Windows o en la ventana del símbolo del sistema 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). Inténtelo más de una vez, ya que el iDRAC6 puede estar ocupado como para aceptar las teclas. La sesión SOL se cerrará.

   NOTA: Si un usuario no finaliza la sesión correctamente, ejecute el siguiente comando para reiniciar el iDRAC. Espere dos minutos hasta que el iDRAC6 se inicie por completo. Para obtener más información, consulte "Generalidades de los subcomandos de RACADM".

   ```
   racadm racreset
   ```

Ejecución de SOL con el proxy SOL

El proxy de comunicación en serie en la LAN (proxy SOL) es un daemon 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 daemon. 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/VT220 o ANSI. Un ejemplo de un emulador de terminal VT100/VT220 o ANSI completo que admite la redirección de consola en el sistema es HyperTerminal Private Edition 6.1 o posterior de Hilgraeve. Además, el uso de la ventana de línea de comandos para ejecutar la redirección de consola serie Telnet puede dar lugar a la aparición de caracteres inservibles.

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 la petición 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, las utilidades de administración de BMC están instaladas en el siguiente directorio en los sistemas operativos Windows:

C:\Archivos de programa\Dell\SysMgt\bmc - (sistema operativo de 32 bits)

C:\Archivos de programa (x86)\Dell\SysMgt\bmc - (sistema operativo de 64 bits)

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 del símbolo del sistema 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 iDRAC6 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 **Expiración de tiempo** de Telnet a cero en la interfaz gráfica web del iDRAC6, en **Sistema→ Acceso remoto→ iDRAC6→ 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→ iDRAC6→ Red/Seguridad→ Red→ Configuración de IPMI→ Clave de cifrado**.

   NOTA: La clave predeterminada de IPMI 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 activada, los valores actuales se muestran y se presentan tres posibilidades:

     1. `Disable Serial-Over-LAN (Deshabilitar la comunicación en serie en la 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 concuerde con la del iDRAC6 y que el usuario cuente con el privilegio de administrador.
   - 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

correcto 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 de los subcomandos de 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 de **/etc/inittab** modificado:

```
_____________________________________________________________________

#

# 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)
```

```
#

OMITIR esta parte del archivo

# 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

OMITIR el resto del archivo
```

Ejemplo de /etc/securetty modificado:

```
Consola
ttyS0
vc/1
vc/2
vc/3
vc/4

OMITIR el resto del archivo
```

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 generated by anaconda (grub.conf generado por anaconda)

#

# Note that you do not have to return grub after making changes to this (Tenga en cuenta que no tiene que volver a ejecutar grub después de hacer cambios en este )

# file (archivo)

# NOTICE: You have a /boot partition. This means that (AVISO: Tiene una partición /boot. Esto significa que)

# all kernel and initrd paths are relative to /boot/, eg. (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

default=0

expiración de tiempo=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 de **/boot/grub/grub.conf** modificado:

```
# grub.conf generated by anaconda (grub.conf generado por anaconda)

#

# Note that you do not have to return grub after making changes to this (Tenga en cuenta que no tiene que volver a ejecutar grub después de hacer cambios en este )

# file (archivo)

# NOTICE: You have a /boot partition. This means that (AVISO: Tiene una partición /boot. Esto significa que)

# all kernel and initrd paths are relative to /boot/, eg. (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

default=0
```

```
expiración de tiempo=5

#splashimage=(hd0,0)/grub/splash.xpm/gz

hiddenmenu


# Redirigir inicio de sistema operativo a través de SOL

title Red Hat Enterprise Linux 5 SOL redirection

     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 UTC 2008 (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###

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 de **/boot/grub/menu.list** modificado en SLES 10:

```
#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###

title SUSE Linux Enterprise Server 10 SP1 SOL redirection

     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 ingresando bootcfg en la ventana del símbolo del sistema 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 del símbolo del sistema 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: Windows Server 2003, Enterprise

      Path: multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

      OS Load Options: /nonexecute=optout /fastdetect /usepmtimer /redirect

_____________________________________________________________________
```

Ejemplo de configuración bootcfg modificada:

```
_____________________________________________________________________

      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

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Esta sección proporciona información acerca de cómo usar la función de redirección de consola del iDRAC6.

Descripción general

La función de redirección de consola del iDRAC6 le permite acceder de manera remota a consolas locales en modo de gráfico o de texto; así, es posible controlar uno o varios sistemas equipados con iDRAC6 desde un solo sitio.

Uso de redirección de consola

La pantalla **Redirección de consola** permite administrar el sistema remoto con el teclado, vídeo y mouse en su estación de administración local para controlar los dispositivos correspondientes en un servidor administrado remoto. Esta característica 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 en cada tarjeta. 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 al menos 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 de que otro usuario tiene el control. El primer usuario debe responder en un lapso de treinta segundos o no se otorgará el acceso al segundo usuario. Cuando hay dos sesiones activas de forma simultánea, el primer usuario ve un mensaje en la esquina superior derecha de la pantalla que identifica al segundo usuario que tiene una sesión activa.

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.

Limpiar el caché del explorador

Si tiene algún problema al operar el vKVM, (errores fuera de rango, problemas de sincronización, etc.) limpie el caché del explorador para quitar/eliminar las versiones anteriores del visor que pueden estar almacenadas en el sistema, e inténtelo de nuevo.

Para limpiar las versiones anteriores del visor Active-X para IE6, haga lo siguiente:

1. Abra el indicador de comandos y cambie el directorio a **Windows\Archivos de programas descargados**.
2. Ejecute **regsvr32 /u VideoViewer.ocx**.
3. Elimine los archivos siguientes: AvctKeyboard.dll, AvctVirtualMediaDE.dll, AvctVirtualMediaES.dll, AvctVirtualMediaFR.dll, AvctVirtualMediaJA.dll, AvctVirtualMediaZH.dll, VideoViewerDE.dll, VideoViewerES.dll, VideoViewerFR.dll, VideoViewerJA.dll, VideoViewerZH.dll y VirtualMediaDLL.dll.
4. Elimine los complementos *Session Viewer* y/o *Video Viewer* que han sido utilizados por Internet Explorer.

Para limpiar versiones anteriores del visor de Active-X para IE7, haga lo siguiente:

1. Cierre el Video Viewer y el explorador de Internet Explorer.
2. Abra el explorador de Internet Explorer nuevamente y vaya a **Internet Explorer→ Herramientas→ Administrar complementos** y haga clic en **Activar o desactivar complementos**. Aparece la ventana **Administrar complementos**.
3. Seleccione **Complementos que han sido utilizados por Internet Explorer** del menú desplegable **Mostrar**.
4. Elimine el complemento *Video Viewer*.

Para limpiar las versiones anteriores del visor Active-X para IE8, haga lo siguiente:

1. Cierre el Video Viewer y el explorador de Internet Explorer.
2. Abra el explorador de Internet Explorer nuevamente y vaya a **Internet Explorer→ Herramientas→ Administrar complementos** y haga clic en **Activar o desactivar complementos**. Aparece la ventana **Administrar complementos**.
3. Seleccione **Todos los complementos** del menú desplegable **Mostrar**.
4. Seleccione el complemento *Video Viewer* y haga clic en el vínculo **Más información**.
5. Seleccione **Quitar** de la ventana **Más información**.
6. Cierre las ventanas **Más información** y **Administrar complementos**.

Para limpiar versiones anteriores del visor de Java® en Windows o Linux, haga lo siguiente:

1. En el indicador de comandos, ejecute `javaws -viewer`
2. Aparece el **Visor del caché de Java**.
3. Elimine el elemento titulado *Cliente de redirección de consola del iDRAC6* y *JViewer*.

También puede ejecutar la función `javaws -uninstall` en el indicador de comandos para quitar todas las aplicaciones del caché.

Resoluciones de pantalla y velocidades de actualización admitidas

La Tabla 11-1 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 11-1. 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 web admitido. Consulte los apartados "Exploradores web admitidos" y "Configuración de un explorador 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. Se recomienda que configure la resolución del monitor en 1280 x 1024 pixeles o más.

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 los 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 / Medios**.
2. Haga clic en **Configuración** para abrir la pantalla **Configuración**.
3. Configure las propiedades de la redirección de consola. La Tabla 11-2 describe la configuración de la redirección de consola.

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

5. Para continuar, haga clic en el botón correspondiente. Consulte Tabla 11-3.

Tabla 11-2. Propiedades de configuración de la redirección de consola

Propiedad	Descripción
Activado	Seleccione esta opción 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**.
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 permitido 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 de mouse	Elija **Windows** si el servidor administrado se esté ejecutando en un sistema operativo Windows®. Elija **Linux** si el servidor administrado ejecuta Linux. Elija **USC/Diagnóstico** si el servidor no está funcionando en un sistema operativo Windows o Linux. **NOTA:** Debe seleccionar **USC/Diagnóstico** en HyperV, Dell Diagnostics o USC (Servicios del sistema). 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 acerca de cómo usar los medios virtuales con la redirección de consola, consulte "Configuración y uso de medios virtuales".

Los botones en Tabla 11-5 están disponibles en la pantalla **Configuración de la redirección de consola**.

Tabla 11-3. Botones de configuración de redirección de consola

Botón	Definición
Imprimir	Imprime la página **Configuración**.
Actualizar	Vuelve a cargar la pantalla **Configuración**.
Aplicar	Guarda todos los nuevos valores de configuración realizados en la redirección de consola.

Abrir una sesión de redirección de consola

Al abrir una sesión de redirección de consola, la aplicación Dell Virtual KVM (vKVM) Viewer (**iDRACView**) se inicia y en el visor aparece el escritorio del sistema remoto. Cuando se usa la aplicación **iDRACView** es posible controlar las funciones del mouse y teclado del sistema remoto desde la estación de administración local.

NOTA: Si vKVM se inicia desde una estación de administración con Windows Vista®, puede emitir mensajes para reiniciarse. Para evitar este problema, defina los valores de tiempo de espera apropiados en las siguientes ubicaciones: **Panel de control→Opciones de energía→Economizador de energía→Configuración avanzada→ Disco duro→ Apagar disco duro tras <tiempo_de_espera>** y **Panel de control→ Opciones de energía→ Alto rendimiento→ Configuración avanzada→ Disco duro→ Apagar disco duro tras <tiempo_de_espera>**.

Para abrir una sesión de redirección de consola en la interfaz web, realice los pasos a continuación:

1. Haga clic en **Sistema→** ficha **Consola / Medios → Redirección de consola y medios virtuales**.

2. En la pantalla **Redirección de consola y medios virtuales**, utilice la información de la Tabla 11-4 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 los medios virtuales en la interfaz web del iDRAC6".

Tabla 11-4. Información sobre redirección de consola

Propiedad	Descripción
Redirección de consola activada	**Sí**/**No**
Cifrado de vídeo activado	**Sí**/**No**
Máx. de sesiones	Muestra el número máximo de sesiones de redirección de consola admitidas.
Sesiones activas	Muestra el número actual de sesiones de redirección de consola activas.
Modo de mouse	Muestra la aceleración actual del mouse. El **Modo de mouse** se debe elegir según 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 distinto a 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**. **NOTA:** Existe la posibilidad de que vKVM no se inicie la primera vez para Internet Explorer 8 si se selecciona **Java** como el tipo de complemento.
Vídeo del servidor local activado	**Sí** indica que la salida al monitor iKVM está activada durante la redirección de consola. **No** indica que las tareas que realice con **Redirección de consola** no se verán en el monitor local del servidor administrado.

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

Los botones en Tabla 11-5 están disponibles en la pantalla **Redirección de consola**.

Tabla 11-5. 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 los 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 el escritorio del sistema remoto aparece en **iDRACView**.

4. Aparecerán dos punteros de mouse en la ventana del visor: Uno para el sistema remoto y otro para el sistema local. Usted deberá sincronizarlos de manera que el puntero remoto siga el puntero local. Consulte "Sincronización de los punteros 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 usted se conecta al 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, acciones de alimentación y acceso a los medios virtuales. Haga clic en **Ayuda** para obtener más información sobre estas funciones.

Cuando usted inicie una sesión de redirección de consola y aparece Video Viewer, es posible que deba ajustar el modo de color y sincronizar los punteros de mouse.

La Tabla 11-6 describe las opciones del menú disponibles en el visor.

Tabla 11-6. 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 del sistema remoto actual en un archivo **.bmp**. Aparece un cuadro de diálogo que permite guardar el archivo en un lugar determinado.
	Pantalla completa	Para expandir el Video Viewer a modo de pantalla completa, haga clic en la esquina superior derecha del visor para obtener la pantalla completa.
	Salir	Cuando haya terminado de usar la consola y haya cerrado la sesión (mediante el procedimiento de desconexión del sistema remoto), seleccione **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.
	Mantener 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 se selecciona una macro o presiona la tecla aceleradora especificada para la macro, la acción se ejecuta en el sistema remoto. Video Viewer ofrece las macros siguientes: • Alt+Ctrl+Supr • Alt+Tab • Alt+Esc • Ctrl+Esc • Alt+Espacio • Alt+Entrar • Alt+Guión • Alt+F4 • ImprPant • Alt+ImprPant • F1 • Pausa • Alt+M • Alt+D • Alt+ImprPant+M • Alt+ImprPant+P
	Paso a través de teclado	El modo de paso a través de teclado permite redirigir todas las funciones del teclado en el cliente al servidor.
Mouse	Sincronizar el cursor	Sincroniza el cursor de modo que el mouse del cliente se redirija al del servidor.
	Ocultar cursor local	Sólo aparecerá el cursor de KVM. Se recomienda esta configuración al ejecutar el 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 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 puede definirse en color de 15 bits y 7 bits.
Alimentación	Encender el sistema	Enciende el sistema.
	Apagar el sistema	Apaga el sistema.
	Apagado ordenado	Apaga el sistema.
	Restablecer el sistema (reinicio mediante sistema operativo)	Reinicia el sistema sin apagarlo.
	Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)	Apaga y luego reinicia el sistema.
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

		ı Unidad flash USB Para obtener información acerca de 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	Acerca de iDRACView	Aparece la versión de iDRACView.

Sincronización de los punteros del mouse

Cuando se conecta a un sistema Dell PowerEdge remoto usando la redirección de consola, la velocidad de aceleración del mouse en el sistema remoto podría no corresponder con la del puntero del mouse en la estación de administración, ocasionando la aparición de dos punteros de mouse en la ventana de Video Viewer.

Para sincronizar los punteros 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 al lado de la opción del menú haya una marca; 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 mouse para Linux antes de iniciar el visor. Consulte "Configuración de la redirección de consola y los medios virtuales en la interfaz web del iDRAC6" para obtener ayuda con la configuración. La configuración predeterminada del mouse del sistema operativo se usa para controlar la flecha del mouse en la pantalla de **Redirección de consola** del iDRAC6.

Desactivación o activación de la consola local

Es posible 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 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: 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/Media** y después haga clic en **Configuración**.
3. Si desea desactivar (apagar) el vídeo local en el servidor, en la pantalla **Configuración** 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** 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.

Inicio de vKVM y medios virtuales de manera remota

Puede iniciar vKVM/medios virtuales ingresando en un URL único en un explorador admitido, en lugar de iniciarlo desde la interfaz gráfica web del iDRAC6. Dependiendo de la configuración de su sistema, deberá pasar por el proceso de autentificación manual (página de inicio de sesión) o será dirigido automáticamente al visor de vKVM/medios virtuales (iDRACView).

NOTA: Internet Explorer admite inicios de sesión locales, Active Directory (AD), tarjeta inteligente (SC) e inicio de sesión único (SSO). Firefox admite inicios de sesión SSO, locales y AD.

Formato del URL

Si escribe el vínculo **https://<ip_del_idrac6>/consola** en el explorador, es probable que deba realizar el proceso de inicio de sesión manual normal, dependiendo de la configuración de inicio de sesión. Si la opción SSO no está activada, y Local, AD o SC sí, aparecerá la página de inicio de sesión correspondiente. Si el inicio de sesión es exitoso, no se iniciará el visor de vKVM/medios virtuales. En su lugar, será redireccionado a la página de inicio de la interfaz gráfica de usuario del iDRAC6.

NOTA: El URL utilizado para iniciar el **iDRACView** distingue entre mayúsculas y minúsculas y deberá ser escrito en minúsculas.

Escenarios de errores generales

Tabla 11-7 enumera los escenarios de errores generales, las razones de estos errores y el comportamiento del iDRAC6.

Tabla 11-7. Escenarios de error

Escenarios de error	Razón	Comportamiento
Falló el inicio de sesión	Ingresó un nombre de usuario inválido o la contraseña incorrecta.	El mismo comportamiento cuando se especifica *https://<ip>* y falla el inicio de sesión.
Privilegios insuficientes	No cuenta con los privilegios de redirección de consola y medios virtuales.	iDRACView no inicia y es redireccionado a la página de la interfaz gráfica de configuración de la consola/medios.
Redirección de consola desactivada	La redirección de consola está desactivada en su sistema.	iDRACView no inicia y es redireccionado a la página de la interfaz gráfica de configuración de la consola/medios.
Se detectaron parámetros del URL desconocidos	El URL que ingresó incluye parámetros indefinidos.	Aparece el mensaje No se encontró la página (404).

Preguntas frecuentes

La Tabla 11-8 contiene las preguntas y respuestas frecuentes.

Tabla 11-8. Uso de la redirección de consola: preguntas frecuentes

Pregunta	Respuesta
vKVM no cierra la sesión cuando se desconecta la interfaz web de usuario fuera de banda.	Las sesiones de vKVM y vMedia se mantienen activas incluso aunque haya finalizado la sesión web. Cierre las aplicaciones de visor vKVM y vMedia para dar por finalizada la correspondiente sesión.
¿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?	Para que el usuario local tenga 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 mouse locales?	Sí.
¿La desactivación de la consola local desactivará el vídeo en la sesión de consola remota?	No, la activación o desactivación del vídeo local es independiente de la sesión de consola remota.
¿Cuáles son los privilegios necesarios para que un usuario del 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 **Redirección de consola y medios virtuales** de la interfaz web del iDRAC6. El comando `racadm getconfig -g cfgRacTuning` de la interfaz de línea de comandos de RACADM muestra el estado en el objeto **cfgRacTuneLocalServerVideo**. Este comando de racadm se puede ejecutar desde Telnet/SSH o una sesión remota al iDRAC6. El comando de RACADM remoto es: `racadm -r <IP_del_iDRAC> -u <usuario> -p <contraseña> getconfig -g cfgRacTuning` 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. Actualice el controlador de vídeo.
¿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 puntero de mouse, lo que ocasiona un retraso en la sincronización. El iDRAC6 tiene un controlador de mouse USB, que permite la posición absoluta y un seguimiento más preciso del puntero de mouse. Aun cuando el iDRAC6 pasara la posición absoluta del mouse USB al BIOS de Dell, la emulación del BIOS lo convertiría nuevamente a la posición relativa y el comportamiento seguiría siendo el mismo. Para solucionar este problema, establezca el modo de mouse en **USC/Diagnóstico** en la pantalla **Configuración**.
¿Por qué no se sincroniza el mouse en la consola de texto de Linux (ya sea en Dell Unified Server Configurator (USC), Dell Lifecycle Controller (LC) o en Dell Unified	El KVM virtual necesita el controlador de mouse USB, pero el controlador de mouse USB sólo está disponible en el sistema operativo X-Window.

Server Configurator Lifecycle Controller Enabled (USC-LCE)?	
Aún tengo problemas con la sincronización del mouse.	Compruebe que el mouse adecuado esté seleccionado para el sistema operativo antes de iniciar una sesión de redirección de consola. Compruebe que **Sincronizar el mouse** esté seleccionado en el menú **Mouse**. Presione <Alt><M> o seleccione **Mouse→ Sincronizar el mouse** para activar/desactivar la sincronización del mouse. Cuando la sincronización esté activada, aparecerá una marca junto a la selección en el menú **Mouse**.
¿Por qué no puedo usar un teclado o mouse mientras instalo un sistema operativo 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. No se 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 aparezca, siempre desactive la redirección de consola en el BIOS antes de instalar un sistema operativo de manera remota.
¿Por qué el indicador de Bloq Num de mi estación de administración no muestra el estado de Bloq Num 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 Num depende de la configuración en el servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Num en la estación de administración.
¿Por qué aparecen varias ventanas de Session Viewer cuándo establezco una sesión de redirección de consola desde el host local?	Usted está configurando una sesión de redirección de consola desde el sistema local. Esto no se permite.
Si ejecuto una sesión de redirección de consola y un usuario local accede al servidor administrado, ¿recibiré un mensaje de advertencia?	No. Si un usuario local tiene acceso al sistema, usted y él tendrán el control del sistema.
¿Cuánto ancho de banda necesito para ejecutar una sesión de redirección de consola?	Se recomienda usar una conexión de 5 MB/seg. para lograr 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 de 500 MHz con 256 MB de RAM como mínimo.

Regresar a la página de contenido

Regresar a la página de contenido

Configuración de una tarjeta del medio VFlash para utilizar con el iDRAC6

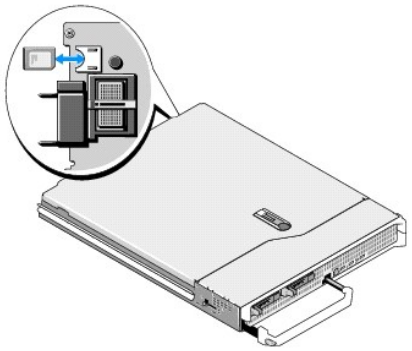
Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

La tarjeta del medio VFlash es una tarjeta Secure Digital (SD) que se conecta en la ranura de la tarjeta opcional del iDRAC6 Enterprise ubicada en la esquina posterior del sistema. La tarjeta proporciona espacio de almacenamiento que actúa como un dispositivo de memoria USB Flash común.

Instalación de una tarjeta del medio VFlash

1. Extraiga el módulo de alta densidad del chasis.
2. Localice la ranura para tarjetas del medio 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 etiqueta hacia arriba, inserte en la ranura para tarjetas 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 del medio VFlash

Para extraer la tarjeta del medio VFlash, presione hacia dentro la tarjeta para soltarla y extráigala de la ranura.

Configuración de la tarjeta del medio VFlash por medio de la interfaz web del iDRAC6

Propiedades de la tarjeta SD

NOTA: Esta sección aparece únicamente si se inserta una tarjeta SD con capacidad de lectura/escritura en la ranura para tarjeta SD del servidor. De lo contrario, aparece el mensaje siguiente:

```
SD card not detected. Please insert an SD card of size 256MB or greater. (No se detectó la tarjeta SD. Inserte una tarjeta SD de 256 MB de tamaño o superior.)
```

1. Asegúrese de que la tarjeta del medio VFlash esté instalada.

2. Abra la ventana del explorador web compatible e 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**.

Tabla 12-1 enumera las opciones de las **Propiedades de la tarjeta SD**.

Tabla 12-1. Propiedades de la tarjeta SD

Atributo	Descripción
Tamaño de la memoria virtual	Le permite seleccionar el tamaño que ocupará la memoria VFlash en la tarjeta SD. Seleccione un tamaño de memoria virtual y haga clic en **Aplicar**. La memoria virtual se reinicializa al tamaño especificado, borra todos los datos existentes y formatea una parte de la tarjeta SD. **NOTA:** Si insertó una tarjeta SD de 1 GB con licencia, puede seleccionar 256 MB ó 512 MB como tamaño de partición. Si insertó una tarjeta SD de cualquier tamaño sin licencia, sólo podrá seleccionar 256 MB como el tamaño de partición. Si cargó una imagen usando WS-MAN, el tamaño de partición máximo que obtiene dependerá del tamaño de la imagen. Por ejemplo, si cargó una imagen de 500 MB, el tamaño de memoria virtual de 1 GB no se podrá crear con una tarjeta de 1 GB con licencia debido a que la imagen ya utiliza 500 MB. En este caso, haga clic en el botón **Inicializar** para reinicializar la tarjeta y seleccione 1 GB como el tamaño de memoria virtual.
Tipo de medios VFlash	Muestra si se insertó una tarjeta SD de Dell o distinta en la ranura para tarjeta SD del servidor. Si la tarjeta SD tiene licencia, aparece la leyenda Dell VFlash seguida del tamaño de la tarjeta SD. Si la tarjeta no tiene licencia, aparece la leyenda Tarjeta SD distinta de Dell.
Imagen	Muestra el nombre del archivo de imagen creado en la tarjeta SD. Se usa como VFlash.
Archivo de identificación	Muestra el nombre del archivo de texto creado en la tarjeta SD. Proporciona información acerca de la imagen VFlash.
Conectar VFlash	Seleccione esta opción para conectar la VFlash. Esto expone el archivo de imagen **ManagedStore.IMG** creado en la tarjeta SD como una memoria USB del tamaño seleccionado. **NOTA:** Puede conectar la VFlash únicamente si hay un archivo de imagen **ManagedStore.IMG** válido en la tarjeta SD.
Inicializar	Haga clic en **Inicializar** para crear el archivo de imagen VFlash **ManagedStore.IMG** en la tarjeta SD. **NOTA:** La opción **Inicializar** sólo está habilitada si hay una tarjeta del medio VFlash. Además, la tarjeta SD sólo puede ser formateada si la opción **Conectar VFlash** no está seleccionada. **NOTA:** Los archivos **ManagedStore.IMG** y **ManagedStore.ID** vistos en la página de la interfaz gráfica para el usuario de VFlash no estarán visibles en el sistema operativo del servidor de host sino en la tarjeta SD.
Aplicar	Guarda la configuración actual. Si modifica el tamaño de memoria virtual por medio del menú desplegable, haga clic en **Aplicar** para crear una nueva memoria virtual con el tamaño especificado. Se borrarán todos los datos existentes. Esta operación puede tardar unos minutos para completarse, dependiendo del tamaño de la memoria virtual seleccionada.

Unidad VFlash

NOTA: La función para cargar un archivo de imagen se encuentra disponible únicamente si hay un archivo de imagen **ManagedStore.IMG** válido en la tarjeta SD y la opción **Conectar VFlash** no está seleccionada.

Tabla 12-2 enumera los valores de configuración de la **unidad VFlash**.

Tabla 12-2. Unidad VFlash

Atributo	Descripción
Archivo de imagen	Seleccione un archivo local en la máquina del cliente para exponerlo como memoria USB VFlash en el servidor remoto. Puede almacenar imágenes de inicio de emergencia y herramientas de diagnóstico directamente en la tarjeta del medio VFlash. El archivo de imagen puede ser una imagen de disco flexible de inicio DOS, como un archivo ***.img** parar Windows® o un archivo **diskboot.img** de los medios Red Hat® Enterprise Linux® para Linux. Puede usar el archivo **diskboot.img** para crear un disco de rescate o un disco para ejecutar instalaciones de red. Puede usar VFlash para alojar una imagen persistente para uso general o de emergencia en el futuro.
Cargar	Haga clic en esta opción para cargar el archivo de imagen seleccionado para la tarjeta SD. Después de completar la carga, el archivo de imagen es almacenado en la tarjeta SD como **ManagedStore.IMG**.

NOTA: Esta versión no admite cargar imágenes ISO y puede generar errores durante la carga.

PRECAUCIÓN: No podrá expulsar la unidad de flash virtual del sistema operativo Windows en el servidor administrado haciendo clic en el botón derecho de la unidad y seleccionando la opción "Expulsar". Para quitar la unidad con seguridad, use la opción proporcionada en la bandeja del sistema en la esquina inferior derecha de su sistema.

Si hace clic en un botón en la página VFlash cuando alguna otra aplicación como proveedor WSMAN, utilidad de configuración del iDRAC6 o RACADM está usando VFlash, el iDRAC6 muestra una página en blanco con el siguiente mensaje `VFlash is currently in use by another process. Try again after some time (Otro proceso está usando actualmente VFlash. Intente de nuevo más tarde.)`

Visualización del tamaño de la memoria flash virtual

El menú desplegable **Tamaño de la memoria virtual** muestra la configuración de tamaño actual.

Configuración de la tarjeta del medio VFlash con RACADM

Activar o desactivar la tarjeta del medio VFlash

Abra una consola local al servidor, inicie sesión e introduzca:

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 ó 0 ]
```

en donde `1` significa activada y `0` significa desactivada.

NOTA: Para obtener más información acerca de cfgRacVirtual, incluidos los detalles de mensajes de salida, consulte "cfgRacVirtual".

Restablecimiento de la tarjeta del medio VFlash

Abra una consola de texto de Telnet/SSH en el servidor, inicie sesión e introduzca:

```
racadm vmkey reset
```

PRECAUCIÓN: Cuando la tarjeta del medio VFlash se restablece con el comando de RACADM, se restablece el tamaño de la memoria en 256 MB y se borran todos los datos existentes.

NOTA: Para obtener más información acerca del comando vmkey, consulte "vmkey". El comando de RACADM sólo funcionará si hay una tarjeta del medio VFlash. Si no hay una tarjeta, aparecerá el siguiente mensaje: *ERROR: No es posible realizar la operación solicitada. Verifique si se insertó una tarjeta SD.*

Regresar a la página de contenido

Regresar a la página de contenido

Configuración y uso de medios virtuales

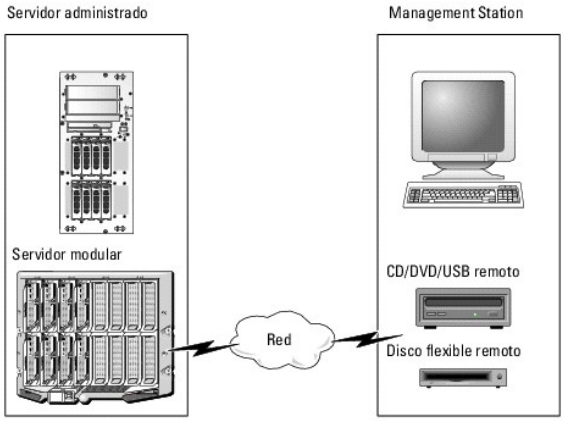
Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

---

Descripción general

La función Medios virtuales, que se 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 13-1 muestra la arquitectura general de los medios virtuales.

Figura 13-1. Arquitectura general de medios virtuales



Por medio de los medios virtuales, los administradores pueden iniciar los servidores administrados, instalar aplicaciones, actualizar controladores o incluso instalar nuevos sistemas operativos de manera remota desde unidades CD/DVD y discos virtuales.

NOTA: Los medios virtuales requieren un ancho 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 otro de disco óptico.

Management Station 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 Management Station por la red. Conectar los medios virtuales se asimila a insertar un medio en un dispositivo físico del sistema administrado. Cuando los medios virtuales están en estado de conexión, los dispositivos virtuales en el sistema administrado aparecen como dos unidades sin los medios instalados.

La Tabla 13-1 enumera las conexiones compatibles de unidades ópticas virtuales y de discos flexibles virtuales.

NOTA: Si cambia los medios virtuales mientras están conectados podría detenerse la secuencia de inicio del sistema.

Tabla 13-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disco virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disco flexible heredada de 1,44 con disco flexible de 1,44	Unidad combinada de CD-ROM, DVD, CD-RW, con medios CD-ROM
Unidad de disco flexible USB con un disco flexible de 1,44	Archivo de imagen de CD-ROM/DVD en el formato ISO9660
Imagen de disco flexible de 1,44	Unidad de CD-ROM USB con medios CD-ROM
Disco USB extraíble (tamaño mínimo de 128 MB)	

Management Station basada en Windows

Para ejecutar la función de medios virtuales en Management Station que está ejecutando el sistema operativo Windows, instale una versión compatible de Internet Explorer con el complemento de control ActiveX. Establezca la seguridad del explorador en el nivel **medio** o en un nivel inferior para permitir que Internet Explorer descargue e instale los controles ActiveX firmados.

Dependiendo de la 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 complementos para ActiveX**, asegúrese de que las siguientes opciones estén fijadas en **Permitir**:
   - Permitir Scriptlets
   - Preguntar automáticamente si se debe usar un control ActiveX
   - Descargar los controles firmados para ActiveX
   - Descargar los controles no firmados para 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 **Opciones de Internet**.
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.

Management Station basada en Linux

Para ejecutar el componente de medios virtuales en una Management Station que está ejecutando el sistema operativo Linux, instale una versión compatible de Firefox.

Para ejecutar el complemento de redirección de consola se requiere Java® Runtime Environment (JRE). Puede descargar JRE desde el sitio **java.sun.com**.

Configuración de los medios virtuales

1. Inicie sesión en la interfaz web del iDRAC6.
2. Haga clic en **Sistema**→ **Consola/Medios**→ **Configuración**.
3. En la sección Medios virtuales, seleccione los valores para la configuración. Consulte Tabla 13-2 para obtener información sobre los valores de configuración de los medios virtuales.
4. 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?)`
5. 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 13-2. 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 ella se pueden conectar múltiples dispositivos. Consulte "Ejecución de los medios virtuales".
Sesiones activas	Muestra la cantidad de sesiones de medios virtuales actualmente activas.
Cifrado activado para medios virtuales	Activa (seleccionada) o desactiva (deseleccionada) el cifrado de las conexiones de Medios virtuales.
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 de medios virtuales aparecerá como dispositivo de disco flexible en el servidor. Cuando se deselecciona, aparece como unidad de memoria USB. **NOTA:** En determinados entornos de Windows Vista® y Red Hat® Enterprise Linux®, existe la posibilidad de que no se pueda virtualizar una unidad USB con la opción **Emulación de disco flexible** activada.
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. Utilice este atributo para iniciar el sistema desde los medios virtuales. En el próximo inicio, el sistema se iniciará desde el siguiente dispositivo en el orden de inicio. Esta opción es útil para implementaciones automáticas.

Ejecución de los medios virtuales

PRECAUCIÓN: No ejecute 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 de la ventana del visor de consola debe permanecer activa mientras accede a los medios virtuales.

1. Abra un explorador web compatible en Management Station.
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 virtualizar como un disco 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 Management Station.

   NOTA: Es posible que los medios virtuales no funcionen correctamente en los clientes con sistema operativo Windows 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 la ventana **Redirección de medios**.

6. Consulte la sección **Estado** en la parte inferior de la ventana **Redirección de medios**. Si hay algún medio conectado, podrá 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.
8. Puede seleccionar el botón de radio **Imagen de disco flexible** y uno de los botones de radio de la sección **Unidad de CD / DVD**.

   NOTA: Si el medio de CD/DVD de Management Station está siendo usado por una tarjeta del iDRAC6, el mismo medio puede redirigirse y ponerse a la disposición de otra tarjeta del iDRAC6. En otras palabras, el iDRAC6 admite la redirección de un mismo medio (sólo lectura) hacia dos tarjetas del iDRAC6 diferentes. Sin embargo, con un medio USB no podrá conectarse a dos tarjetas del iDRAC6. El iDRAC6 muestra un mensaje de advertencia que indica lo mismo.

   Para conectar una imagen de disco flexible o una imagen ISO, introduzca la ruta de acceso a la ubicación de la imagen en su equipo local o haga clic en el botón **Examinar** para desplazarse hasta la ubicación de la imagen.

NOTA: No podrá montar imágenes ISO remotas si utiliza el complemento Java de medios virtuales. Por ejemplo, los clientes Linux no le permitirán montar las imágenes debido a que usan el complemento Java. Para evitar este problema, copie la imagen ISO en el sistema local de modo que el archivo de imagen esté disponible de forma local. El complemento Java de medios virtuales no le permite especificar el nombre del recurso compartido mediante el formato **\\computer\share**.

9. Haga clic en el botón **Conectar que se encuentra junto a cada tipo de medio seleccionado.**

   Los medios están conectados y la ventana de **estado** se actualiza.

10. Haga clic en **Cerrar.**

NOTA: Siempre que se inicia una sesión de medios virtuales o se conecta una unidad VFlash, aparece una unidad adicional denominada "LCDRIVE" en el sistema operativo del host y el BIOS. La unidad adicional desaparece cuando la unidad VFlash o la sesión de medios virtuales se desconectan.

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.

   Los medios se desconectarán y se actualizará la ventana de **estado**.

3. Haga clic en **Cerrar**.

NOTA: Cuando inicia **iDRACview** y luego se desconecta de la interfaz web del usuario, **iDRACView** no finaliza y permanece activo.

Inicio desde los medios virtuales

El BIOS del sistema le permite iniciar desde unidades ópticas virtuales o desde unidades de disco 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 ópticas virtuales y de discos virtuales con los dispositivos estándar de inicio.

4. Asegúrese de que la unidad virtual esté activada y que aparezca como el primer dispositivo con un medio de inicio. 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 de inicio con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio de inicio 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 de inicio.

Instalación de sistemas operativos mediante medios virtuales

Esta sección describe un método manual e interactivo para instalar el sistema operativo en Management Station 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 "Implementación del sistema operativo" para obtener más información.

1. Verifique lo siguiente:
   - El DVD/CD de instalación del sistema operativo está insertado en la unidad de DVD/CD de Management Station.
   - 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 desde 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 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 basados en 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 13-3 contiene preguntas y respuestas frecuentes.

Tabla 13-3. 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 admitidos.
¿Qué exploradores web son compatibles con el iDRAC6?	Consulte "Exploradores web admitidos" para ver una lista de los exploradores 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, el 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 si 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 instala el sistema operativo Windows y la conexión de red es lenta, es posible que la instalación requiera más tiempo 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 virtual. Cierre la aplicación utilizada para ver el contenido de la unidad antes de que intente hacer virtual la unidad.
¿Cómo configuro mi dispositivo virtual como dispositivo de inicio?	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 VFlash y cambie el orden de inicio de dispositivo según sea necesario. Por ejemplo, para iniciar a partir de una unidad de CD, configure ésta como la primera unidad en el orden de inicio.
¿Desde qué tipos de medios puedo iniciar el sistema?	El iDRAC6 permite iniciar a partir de los siguientes medios de inicio: • Medios de CDROM/DVD de datos • Imagen ISO 9660 • Imagen de disco flexible o disco flexible de 1,44 • 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 de inicio?	Busque en **support.dell.com** la utilidad Dell Boot Utility, un programa para Windows que se puede usar para que la memoria USB de Dell funcione como dispositivo de inicio. 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 de petición de comando DOS, introduzca el comando siguiente: sys a: *x*: /s donde *x*: es la memoria USB que desea hacer de inicio.
¿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 del 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.
No puedo encontrar el dispositivo de disco 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 virtual y la unidad de CD virtual de manera similar. Para montar la unidad de disco virtual, localice el nodo de dispositivo que Linux asigna a la unidad de disco virtual. Realice los pasos a continuación para encontrar y montar correctamente la unidad de disco virtual: 1. Abra una ventana de símbolo del sistema de Linux y ejecute el siguiente comando: grep "Disco virtual" /var/log/messages 2. Localice la última entrada de dicho mensaje y anote la hora. 3. En la ventana de petición de comando 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 de que está conectado a la unidad de disco virtual. 6. En la ventana de petición de comando de Linux, ejecute el siguiente comando: mount */dev/sdx* /mnt/floppy donde: */dev/sdx* es el nombre del dispositivo que se encontró en el paso 4 /mnt/floppy es el punto de montaje.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos de RACADM

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

La interfaz de línea de comandos (CLI) de RACADM brinda acceso a las funciones de administración del iDRAC6 en el servidor administrado. RACADM permite acceder a la mayoría de las funciones de la interfaz web del iDRAC6. RACADM se puede usar con secuencias de comandos para facilitar la configuración de varios servidores en lugar de usar la interfaz web, que es más útil para la administración interactiva.

Las siguientes interfaces están disponibles para RACADM:

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

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. RACADM remoto es una utilidad en el lado del cliente que puede ejecutarse desde una estación de administración a través de la interfaz de red fuera de banda. RACADM SSH/Telnet se utiliza para hacer referencia al uso del comando RACADM desde una petición de SSH o Telnet.

En esta sección se proporciona la información siguiente:

- Comandos RACADM e interfaces admitidas de RACADM
- Uso de RACADM local desde una petición de comandos
- RACADM remoto
- RACADM SSH/Telnet
- Configuración del iDRAC6 por medio del comando **racadm**
- Uso del archivo de configuración de RACADM para configurar varios iDRAC6

PRECAUCIÓN: El firmware más reciente del iDRAC6 admite únicamente la versión más reciente de RACADM. Es posible que encuentre errores si utiliza una versión anterior de RACADM para consultar el iDRAC6 que tiene el firmware más reciente. Instale la versión de RACADM que se incluye con el DVD Dell™ OpenManage™ más reciente.

Subcomandos de RACADM

Tabla 14-1 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 de los subcomandos de RACADM".

Tabla 14-1. Subcomandos de RACADM

Comando	Descripción
arp	Muestra el contenido de la tabla ARP. Los registros de la tabla ARP no se pueden agregar ni eliminar.
clearasrscreen	Borra la pantalla de último bloqueo (ASR).
coredump	Muestra el último volcado central del iDRAC6.
coredumpdelete	Borra el volcado de central almacenado en el iDRAC6.
clrraclog	Borra el registro del 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.
fwupdate	Actualiza el firmware del 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.
getsel	Muestra las entradas del registro de sucesos del sistema.
getssninfo	Muestra información sobre las sesiones activas.
getsvctag	Muestra la etiqueta 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 del iDRAC6. Si se usa con -i, el comando muestra el número de anotaciones en el registro de rastreo del iDRAC6.
help	Enumera los subcomandos del iDRAC6.
help <*subcomando*>	Muestra la descripción de uso del subcomando especificado.
ifconfig	Muestra el contenido de la tabla de interfaz de red.
krbkeytabupload	Permite cargar un archivo keytab de Kerberos.
localconredirdisable	Desactiva el kVM local desde el sistema local.
netstat	Muestra la tabla de enrutamiento y las conexiones actuales.
ping	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se requiere una dirección IP de destino. Se envía un paquete de eco de ICMP a la dirección IP de destino en función del contenido de tabla de enrutamiento actual.
ping6	Verifica que se pueda acceder a la dirección IPv6 de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se requiere una dirección IPv6 de destino. Se envía un paquete de eco de ICMP a la dirección IPv6 de destino en función del contenido de la tabla de enrutamiento actual.
racdump	Muestra información general y del estado del iDRAC6.
racreset	Restablece la configuración del iDRAC6.
racresetcfg	Restablece la configuración predeterminada del iDRAC6.
remoteimage	Recurso de archivos compartidos remoto.
serveraction	Realiza operaciones de administración de alimentación en el servidor administrado.
setniccfg	Establece la configuración IP para el controlador.
sshpkauth	Le permite cargar un máximo de 4 claves públicas SSH diferentes, eliminar claves existentes y ver las claves que ya se encuentran en el iDRAC6.
sslcertdownload	Descarga un certificado de 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 de la NIC del iDRAC6.
testtrap	Obliga al iDRAC6 a enviar una alerta SNMP a través de la NIC del iDRAC6.
traceroute	Rastrea la ruta de red de enrutadores que toman los paquetes a medida que se reenvían desde el sistema hasta una dirección IPv4 de destino.
traceroute6	Rastrea la ruta de red de enrutadores que los paquetes toman a medida que se envían desde el sistema hasta una dirección IPv6 de destino.
version	Muestra la información de versión del iDRAC6.
vmdisconnect	Cierra todas las conexiones de medios virtuales del iDRAC6 desde los clientes remotos.
vmkey	Restablece la partición de VFlash al tamaño predeterminado de 256 MB y elimina todos los datos de la partición.

Interfaces admitidas de RACADM

La Tabla 14-2 contiene una descripción general de los subcomandos de RACADM y su compatibilidad correspondiente con interfaces.

Tabla 14-2. Compatibilidad de interfaces de los subcomandos de RACADM

Subcomando	Telnet/SSH	RACADM local	RACADM remoto
arp	✔	✘	✔
clearasrscreen	✔	✔	✔
clrraclog	✔	✔	✔
clrsel	✔	✔	✔
config	✔	✔	✔
coredump	✔	✔	✔
coredumpdelete	✔	✔	✔
fwupdate	✔	✔	✔
getconfig	✔	✔	✔
getniccfg	✔	✔	✔
getraclog	✔	✔	✔
getractime	✔	✔	✔

getsel	✓	✓	✓
getssninfo	✓	✓	✓
getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
krbkeytabupload	✗	✓	✓
localconredirdisable	✗	✓	✗
netstat	✓	✗	✓
ping	✓	✗	✓
ping6	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
remoteimage	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sshpkauth	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✓ (sólo genera, no descarga)	✓	✓
sslkeyupload	✗	✗	✗
testemail	✓	✓	✓
testtrap	✓	✓	✓
traceroute	✓	✗	✓
traceroute6	✓	✗	✓
usercertupload	✗	✗	✗
usercertview	✗	✗	✗
version	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓
✓ = compatible; ✗ = no compatible			

Uso de comandos de RACADM local

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, inicie un shell de comandos e introduzca comandos de RACADM local en alguno de los siguientes formatos:

- `racadm <subcomando> [parámetros]`
- `racadm <getconfig|config> [-g <grupo>] [-o <objeto> <valor>]`

Sin opciones, el comando de RACADM muestra la información general de uso. Para mostrar la lista de subcomandos de RACADM, introduzca:

```
racadm help
```

O bien:

```
racadm getconfig -h
```

La lista de subcomandos incluye todos los comandos de RACADM 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.

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 Enterprise" 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.

Cómo agregar un usuario del 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 al usuario.

Ejemplo

El ejemplo a continuación describe cómo agregar un nuevo usuario de nombre "Juan" con una contraseña "123456" y privilegios de inicio de sesión en el iDRAC6.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 juan

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -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 Tabla 14-3:

Tabla 14-3. Máscaras de bits para privilegios del usuario

Privilegio de usuario	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

Por ejemplo, para permitir al usuario **Configurar el iDRAC6**, **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
```

Carga, visualización y eliminación de claves SSH por medio de RACADM

Cargar

El modo de carga permite cargar un archivo de clave o copiar el texto de la clave en la línea de comandos. No es posible cargar y copiar una clave al mismo tiempo.

En RACADM local:

```
racadm sshpkauth -i <2 a 16> -k <1 a 4> -f <nombre_de_archivo>
```

En RACADM de Telnet/SSH:

```
racadm sshpkauth -i <2 a 16> -k <1 a 4> -t

<texto-de-la-clave>
```

Ejemplo:

Cargue una clave válida en el usuario 2 de iDRAC6 en el primer espacio de clave por medio de un archivo:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

El archivo de clave de autenticación PK SSH se cargó correctamente en el RAC.

PRECAUCIÓN: La opción "archivo" no se admite en el RACADM de Telnet/SSH/Serie.

Vista

El modo de visualización permite al usuario ver una clave que haya especificado o todas las claves.

```
racadm sshpkauth -i <2 a 16> -v -k <1 a 4>

racadm sshpkauth -i <2 a 16> -v -k all
```

Delete

El modo de eliminación permite al usuario eliminar una clave que haya especificado o todas las claves.

```
racadm sshpkauth -i <2 a 16> -d -k <1 a 4>

racadm sshpkauth -i <2 a 16> -d -k all
```

PRECAUCIÓN: La capacidad de cargar, ver y/ o eliminar claves SSH depende del privilegio del usuario "Configurar usuarios". Este privilegio permite a los usuarios configurar la clave SSH de cualquier otro usuario. Dada la importancia de las claves SSH, controle con sumo cuidado la asignación de este privilegio.

Consulte "sshpkauth" para obtener información sobre las opciones de subcomandos.

Eliminación de un usuario del 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 al usuario 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
```

(-i 2 corresponde a la entrada del índice n.º 2 en la tabla de alertas de correo electrónico)

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 del 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
```

(-i 2 corresponde a la entrada del índice n.º 2 en la tabla de alertas de correo electrónico)

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 los subcomandos **testtrap** y **testemail** para configurar estos valores. Consulte "Configuración de capturas de sucesos de plataforma (PET)" para obtener más información.

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 activar esta función:

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

Los comandos proporcionan la misma funcionalidad de configuración que la utilidad de configuración del iDRAC6 cuando se le pide que presione <Ctrl><E>. Para obtener más información sobre la configuración de las propiedades de red con la utilidad de configuración del iDRAC6, consulte "LAN del 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 MI_DOMINIO
```

NOTA: Si **cfgNicEnable** se define en **0**, la LAN del 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 de IPMI 2.0.

   a. Actualice los privilegios de canal de IPMI con el comando siguiente:

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

      donde <*nivel*> es uno de los siguientes valores:

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

      Por ejemplo, para establecer el privilegio de canal de LAN de IPMI 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 del 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 de IPMI 2.0.

   a. Actualice el nivel mínimo de privilegio de la SOL de IPMI con el comando siguiente:

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <nivel>
      ```

      donde <*nivel*> es uno de los siguientes:

      - 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 (SOL) 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 ó 115200 bps.

      Por ejemplo:

      ```
      racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
      ```

   c. Active la comunicación en serie en la LAN escribiendo el comando siguiente en el símbolo del sistema.

   NOTA: Es posible activar o desactivar la SOL para cada usuario individual.

   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable 1 -i <identificación>
   ```

   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. Tabla 14-4 muestra las acciones posibles y el valor para identificarlas en RACADM.

Tabla 14-4. Acción de sucesos de plataforma

Acción	Valor
Sin acción	0
Apagado	1
Reiniciar	2
Ciclo de encendido	3

Configure las acciones de filtro de sucesos de plataforma (PEF) 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 5-8) y <*valor_de_acción*> es un valor de Tabla 14-4.

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` ó `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 símbolo del sistema, 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 el servidor SMTP de correo electrónico, introduzca el siguiente comando:

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <dirección IP del servidor SMTP de correo electrónico>
   ```

5. 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.

6. 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 del filtro de IP (Rango de IP)

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 **cfgRacTuning**.

Tabla 14-5. 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 inicie sesión cualquier dirección IP que contenga este patrón de bits en los bits superiores. Fallarán los inicios de sesión que provengan de las direcciones IP que estén fuera de este rango. 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.

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" para obtener más información sobre RACADM y los comandos de RACADM.

1. Los siguientes comandos de 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 incluyen:

- 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: 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 Enterprise" 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 14-6. 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 un lapso de tiempo específico (**cfgRacTuneIpBlkFailWindow**), todos los intentos posteriores de establecimiento de sesión que provengan de dicha dirección serán rechazados durante un periodo 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 periodo 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 periodo 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 de sesión 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 3600
```

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 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 del 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 23 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".

RACADM SSH / Telnet y remoto

RACADM remoto es una utilidad en el lado del cliente que puede ejecutarse desde una estación de administración a través de la interfaz de red fuera de banda. Se proporciona una opción de capacidad remota (**-r**) que le permite conectarse al sistema administrado y ejecutar subcomandos de RACADM desde una consola remota o una estación de administración. Para usar la capacidad remota, necesita un nombre de usuario válido (opción **-u**) y una contraseña (opción **-p**), así como la dirección IP del iDRAC6. RACADM SSH/Telnet se utiliza para hacer referencia al uso del comando de RACADM desde un símbolo del sistema SSH o Telnet.

La cantidad máxima de sesiones simultáneas de RACADM remoto es cuatro. Estas sesiones son independientes y adicionales a las sesiones de Telnet y SSH. El iDRAC6 puede admitir simultáneamente cuatro sesiones SSH y cuatro sesiones de Telnet, además de las cuatro sesiones de RACADM.

NOTA: Configure la dirección IP en el iDRAC6 antes de usar la capacidad remota de RACADM.

NOTA: Si el sistema desde el que está accediendo al sistema remoto no tiene un certificado de iDRAC6 en el almacén predeterminado de certificados, aparecerá un mensaje cuando escriba un comando de RACADM.

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (Alerta de seguridad: El certificado no es válido; el nombre que aparece en el certificado no es válido o no coincide con el nombre del sitio)

Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors. (Ejecución continua. Utilice la opción -S para que racadm detenga la ejecución al producirse errores relacionados con certificados.)
```

RACADM continúa ejecutando el comando. No obstante, si utiliza la opción `-S`, RACADM detendrá la ejecución del comando y mostrará el siguiente mensaje:

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name (Alerta de seguridad: El certificado no es válido; el nombre que aparece en el certificado no es válido o no coincide con el nombre del sitio)

Racadm not continuing execution of the command. (Racadm detiene la ejecución del comando.)

ERROR: Unable to connect to iDRAC6 at specified IPaddress (ERROR: No es posible establecer conexión con el iDRAC6 en la dirección IP especificada)
```

NOTA: Al utilizar la capacidad remota de RACADM, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos de RACADM que involucran operaciones de archivos, por ejemplo:

```
racadm getconfig -f <nombre de archivo>
```

O bien:

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

Uso de RACADM remoto

```
racadm -r <dirección IP del iDRAC6> -u <nombre de usuario> -p <contraseña> <subcomando> <opciones del subcomando>

racadm -i -r <dirección IP del iDRAC6> <subcomando> <opciones del subcomando>
```

Por ejemplo:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo

racadm -i -r 192.168.0.120 getsysinfo
```

Si el número de puerto HTTPS del iDRAC6 se ha cambiado a un puerto personalizado diferente al predeterminado (443), se debe utilizar la siguiente sintaxis:

```
racadm -r <dirección IP del iDRAC6>:<puerto> -u <nombre_de_usuario> -p <contraseña> <subcomando> <opciones del subcomando>

racadm -i -r <dirección IP del iDRAC6>:<puerto> <subcomando> <opciones del subcomando>
```

Opciones de RACADM remoto

La Tabla 14-7 muestra las opciones para los comandos de RACADM remoto.

Tabla 14-7. Opciones de comandos de RACADM

Opción	Descripción
-**r <***dirección IP del RAC***>** -**r <***dirección IP del RAC***>:<***número de puerto***>**	Especifica la dirección IP remota del controlador. Use *<número de puerto>* si el número de puerto del iDRAC6 no es el puerto predeterminado (443)
-**i**	Indica a RACADM que pregunte interactivamente al usuario el nombre de usuario y la contraseña.
-**u <***Nombre de usuario***>**	Especifica el nombre de usuario que se usa para autentificar la transacción del comando. Si se usa la opción **-u**, se debe usar la opción **-p**, y la opción **-i** (interactiva) no se permite.
-**p <***contraseña***>**	Especifica la contraseña usada para autentificar la transacción del comando. Si se usa la opción **-p**, la opción **-i** no se permite.
-S	Indica que RACADM debe verificar si existen errores por certificados no válidos. RACADM detiene la ejecución del comando y muestra un mensaje de error si detecta un certificado no válido.

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 editar entonces el archivo y usar el subcomando **config -f** de RACADM para volver a cargar el archivo en el iDRAC6 o para copiar la configuración a otros iDRAC6.

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 siguiente comando:

```
racadm -r <IP de iDRAC6 remoto> -u <usuario> -p <contraseña> 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 del 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* comenzar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de configuración se organizan en grupos según se define en "Definiciones de grupos y objetos de la base de datos de propiedades del iDRAC6 Enterprise".

  El siguiente ejemplo muestra un nombre de grupo, el objeto y el valor de propiedad del objeto.

  Ejemplo:

  ```
  [cfgLanNetworking] (nombre de grupo)

  cfgNicIpAddress=192.168.1.1 (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 entrada 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-único>.`

- 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 <indice> ""
  ```

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 <indice>
  ```

- 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 del 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 entradas 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 bien 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:

```
#

# Grupo de objeto "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Este archivo será actualizado de la siguiente manera:

```
#

# 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 actualice al iDRAC6.

NOTA: Use el subcomando **racresetcfg** para restablecer la base de datos y la configuración de la tarjeta de interfaz de red del iDRAC6 a los valores predeterminados originales y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario "root" está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Antes de 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 siguiente comando:

```
racadm -r <IP de iDRAC6 remoto> -u <usuario> -p <contraseña> config -f myconfig.cfg
```

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 iDRAC6

A través de un archivo de configuración, usted puede configurar otros iDRAC6 con propiedades idénticas. Siga estos pasos para configurar varios iDRAC6:

1. Cree el archivo de configuración del iDRAC6 cuyos valores desea copiar en los demás. Introduzca el comando siguiente:

   ```
   racadm -r <IP de iDRAC6 remoto> -u <usuario> -p <contraseña> getconfig -f <nombre de archivo>
   ```

   donde <*nombre de archivo*> es el nombre de un archivo para guardar las propiedades del iDRAC6, como **myconfig.cfg**.

   El ejemplo a continuación muestra cómo es posible usar comandos de RACADM remoto para configurar varios iDRAC6. Cree un archivo de procesamiento en lote en la estación de administración y ejecute los comandos de RACADM remoto desde el archivo de proceso por lotes.

   Por ejemplo:

   ```
   racadm -r <IP 1 de servidor> -u <usuario> -p <contraseña> config -f myconfig.cfg

   racadm -r <IP 2 de servidor> -u <usuario> -p <contraseña> config -f myconfig.cfg

   ...
   ```

   Consulte "Creación de un archivo de configuración de iDRAC6" para obtener más información.

   NOTA: Algunos archivos de configuración contienen información exclusiva del iDRAC6 (como la dirección IP estática) que debe modificarse antes de exportar el archivo a otros iDRAC6.

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 un símbolo del sistema.

   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 -r <IP de iDRAC6 remoto> -u <usuario> -p <contraseña> 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 WS-MAN

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Web Services for Management (WS-MAN) es un protocolo basado en SOAP (Protocolo simple de acceso a objetos), utilizado en la administración de sistemas. WS-MAN proporciona un protocolo con capacidad interoperable para dispositivos para poder compartir e intercambiar datos a través de redes. El iDRAC6 utiliza WS-MAN para transmitir información de administración basada en el modelo común de información (CIM) del Grupo de trabajo de administración distribuida (DMTF); la información del CIM define la semántica y los tipos de información que pueden manipularse en un sistema administrado. Las interfaces incorporadas por Dell™ para administración de plataforma del servidor se organizan en perfiles, cada uno de los cuales define las interfaces específicas para cada dominio de administración o área de funcionalidad en particular. Además, Dell ha definido diversas extensiones de modelo y perfil que ofrecen interfaces para otras capacidades.

Los datos que se encuentran disponibles a través de WS-MAN son provistos por la interfaz de instrumentación del iDRAC6 asignada a los perfiles de DMTF y de extensión de Dell.

Funciones de WS-Management

La especificación WS-Management promueve la interoperabilidad entre aplicaciones de administración y recursos administrados. Al identificar un conjunto principal de especificaciones de servicios web y requisitos de uso para exhibir un conjunto común de operaciones centrales para la administración de todos los sistemas, WS-Management es capaz de hacer lo siguiente:

- DETECTAR la presencia de recursos administrados y trasladarse entre ellos
- OBTENER, ESTABLECER, CREAR Y ELIMINAR recursos individuales de administración, como configuraciones y valores dinámicos
- ENUMERAR el contenido de contenedores y recopilaciones, como registros y tablas de gran tamaño
- EJECUTAR métodos específicos de administración con parámetros de entrada y salida con establecimiento inflexible de tipos

---

Perfiles CIM admitidos

Tabla 17-1. Perfiles CIM admitidos

DMTF estándar
1. Servidor básico Define las clases de CIM para representar el servidor host.
2. Medidas básicas Define las clases de CIM para ofrecer la capacidad de modelar y controlar las métricas capturadas para elementos administrados.
3. Procesador de servicio Define las clases de CIM para modelar procesadores de servicio.
4. Redirección de USB Define las clases de CIM para describir información acerca de las redirecciones de USB. Para dispositivos de teclado, vídeo y mouse, este perfil debe usarse si los dispositivos se administrarán como dispositivos USB.
5. Propiedad física Define las clases de CIM para representar el aspecto físico de los elementos administrados. El iDRAC6 usa este perfil para representar la información de FRU del servidor host y de sus componentes, además de la tipología física.
6. Admin de dominios SM-CLP Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del CLP.
7. Administración del estado de la alimentación Define las clases de CIM para las operaciones de control de alimentación. El iDRAC6 usa este perfil para las operaciones de control de alimentación del servidor host.
8. Servicio CLP Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del CLP.
9. Interfaz IP Define las clases de CIM para representar la interfaz IP de un sistema administrado.
10. Cliente DHCP Define las clases de CIM para representar un cliente DHCP y sus funciones y configuración asociadas.
11. Cliente DNS

Define las clases de CIM para representar un cliente DNS en un sistema administrado.
12. Registro Define las clases de CIM para representar distintos tipos de registros. El iDRAC6 usa este perfil para representar el registro de sucesos del sistema (SEL) y el registro RAC del iDRAC6.
13. Autorización basada en funciones Define las clases de CIM para representar funciones. El iDRAC6 usa este perfil para configurar privilegios de la cuenta iDRAC6.
14. Recopilación SMASH Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del CLP.
15. Registro de perfiles Define las clases de CIM para anunciar las implementaciones de perfil. El iDRAC6 usa este perfil para anunciar sus propios perfiles implementados, como se describe en esta tabla.
16. Administración de identidad simple Define las clases de CIM para representar identidades. El iDRAC6 usa este perfil para la configuración de cuentas iDRAC6.
17. Puerto Ethernet Define las clases de CIM para representar un puerto Ethernet, su controlador asociado y las interfaces Ethernet en un sistema administrado. Las asociaciones con los aspectos físicos del puerto y la información de la versión de la implementación del perfil se modelan en este perfil.
18. Sensor Define las clases de CIM utilizadas para describir los sensores en un sistema administrado. También define las clases de asociaciones que describen la relación de los sensores con los dispositivos supervisados.
Extensiones de Dell
1. Cliente Active Directory Define las clases de extensiones de CIM y Dell para configurar el cliente iDRAC6 Active Directory y los privilegios locales para grupos de Active Directory.
2. Medios virtuales Define las clases de extensiones de CIM y Dell para configurar los medios virtuales del iDRAC6. Extiende el perfil de *redirección de USB*.
3. Implementación de sistema operativo Define las clases de extensión de CIM y Dell para representar la configuración de las funciones de implementación de sistema operativo. Amplía la función de administración de hacer referencia a los perfiles al sumar la compatibilidad con actividades de implementación de sistema operativo manipulando las funciones de ese tipo de implementación que ofrece el procesador de servicio.
4. Inventario de software Define las extensiones de Dell y CIM para representar las versiones actualmente instaladas del BIOS, firmware de componentes, diagnósticos, Unified Server Configurator y de los paquetes Driver Pack de controladores. Asimismo, brinda una representación de las versiones de las imágenes de actualización del BIOS y el firmware que se encuentran disponibles en Lifecycle Controller para reversión y reinstalación.
5. Actualización de software Define las extensiones de CIM y Dell para la representación de los métodos y la clase de servicio para actualizar el BIOS, diagnósticos, paquete de controladores y firmware de componentes y Lifecycle Controller. Los métodos de actualización admiten la actualización desde ubicaciones de red compartidas CIFS, NFS, FTP y HTTP y desde las imágenes de actualización situadas en Lifecycle Controller. Las solicitudes de actualización se emiten como trabajos y pueden programarse de inmediato o posteriormente con varias opciones de tipos de acciones de reinicio para aplicar las actualizaciones.
6. Control de trabajos Define las extensiones de CIM y Dell para la administración de los trabajos generados por las solicitudes de actualización. Los trabajos pueden crearse, eliminarse, modificarse y agregarse a colas de espera de trabajos para establecer una secuencia y ejecutar múltiples actualizaciones en un solo reinicio.
7. Administración de LC Define las extensiones de CIM y Dell que permiten obtener y definir los atributos para administrar las funciones de descubrimiento automático y reemplazo de piezas del controlador Lifecycle Controller.

La implementación de WS-MAN del iDRAC6 utiliza SSL en el puerto 443 para garantizar la seguridad de transporte y admite autenticación básica y de resumen. Las interfaces de servicios web se pueden utilizar aprovechando la infraestructura cliente, como la CLI de WinRM y Powershell de Windows®, utilidades de código fuente abierto como WSMANCLI y entornos de programación de aplicaciones como Microsoft® .NET®.

Se ofrecen guías de implementación adicionales, documentos técnicos, muestras de perfiles y códigos, disponibles en Dell Enterprise Technology Center en **www.delltechcenter.com**. Para obtener más información, consulte también:

- Sitio web de DTMF: **www.dmtf.org/standards/profiles/**
- Notas de publicación o archivo léame de WS-MAN.

Regresar a la página de contenido

Regresar a la página de contenido

Uso de la interfaz de línea de comandos SM-CLP de iDRAC6 Enterprise

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Esta sección brinda 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 con las especificaciones de SM-CLP de SMWG. Para obtener más información sobre estas especificaciones, visite el sitio web del Grupo de trabajo de administración distribuida (DMTF) en **www.dmtf.org**.

El SM-CLP de iDRAC6 es un protocolo impulsado por DMTF y SMWG para proporcionar estándares para las implementaciones de la interfaz de línea de comandos (CLI) 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 el 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™, mientras que SM-CLP es una interfaz estándar de la industria.

NOTA: Para obtener información sobre la base de datos de propiedades SM-CLP del iDRAC6, la asignación entre clases WS-MAN y destinos SM-CLP, y detalles sobre la implementación de Dell, consulte los documentos *Asignación de elementos CIM de iDRAC6* y *Base de datos de propiedades del iDRAC6 SM-CLP*, disponibles en Dell Enterprise Technology Center en **www.delltechcenter.com**. La información incluida en el documento *Asignación de elementos CIM de iDRAC6* se especifica en los perfiles de DMTF. Las estructuras WS-MAN se documentan en los perfiles de DMTF y los MOF disponibles en **http://www.dmtf.org/standards/profiles/**. Además, las extensiones de Dell están disponibles en **http://www.delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions**.

Administración del sistema por medio de SM-CLP

El SM-CLP del iDRAC6 permite administrar las siguientes funciones de sistema desde una línea de comandos:

- Administración de la alimentación de servidor: Enciende, apaga o reinicia el sistema
- Administración de registro de sucesos del sistema (SEL): 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

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 del iDRAC6 está basada en la versión 1.0 de la especificación SM-CLP proporcionada por DMTF.

Las siguientes secciones proporcionan una descripción de la característica de SM-CLP que se aloja en el iDRAC6.

NOTA: Si estableció una sesión SM-CLP a través de Telnet/SSH y la sesión no se cierra correctamente debido a una desconexión de la red, es posible que se muestre un mensaje de error para indicar que alcanzó la cantidad máxima de conexiones. Para resolver este problema, termine la sesión SM-CLP en la interfaz gráfica de usuario web en **Sistema→ Acceso remoto→ iDRAC6→ Red/Seguridad→ Sesiones** antes de intentar establecer una nueva sesión.

NOTA: El iDRAC6 admite hasta 4 sesiones de Telnet y 4 sesiones de SSH simultáneamente. No obstante, sólo *una* de las 8 sesiones posibles puede usar SM-CLP. Es decir, el iDRAC6 admite solamente una sesión SM-CLP a la vez.

Cómo iniciar una sesión SM-CLP

- Conéctese al iDRAC6 a través de SSH/Telnet para ir a la interfaz de línea de comandos (consola).
- Escriba "smclp" en la solicitud del símbolo de dólar para iniciar la consola SM-CLP.

Sintaxis:

```
telnet <dirección_IP_iDRAC6>
```

```
$; (se muestra la solicitud de la interfaz de línea de comandos)

$smclp; (en la solicitud de la interfaz de línea de comandos, escriba smclp)
```

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, mientras que el destino es la entidad (u objeto) en la que se ejecuta dicha operación.

A continuación se presenta la sintaxis de la línea de comandos de SM-CLP:

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

La Tabla 16-1 muestra una lista de verbos compatibles con la CLI del iDRAC6, la sintaxis de cada comando y una lista de opciones compatibles con el verbo.

Tabla 16-1. Verbos compatibles con la CLI de SM-CLP

Verbo	Descripción	Opciones
cd	Se desplaza 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
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
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 subdestinos 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

Tabla 16-2 describe las opciones de SM-CLP. Algunas opciones están en forma abreviada, según se muestra en la tabla.

Tabla 16-2. Opciones admitidas por SM-CLP

Opción de SM-CLP	Descripción
-all, -a	Indica al verbo que va a realizar todas las funciones posibles.
-destination	Especifica la ubicación para almacenar 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 va a validar la sintaxis del comando sin ejecutarlo.
-help, -h	Muestra la ayuda del verbo.
-level, -l	Indica al verbo que opere en destinos de niveles adicionales debajo del destino especificado. Sintaxis: -level <*n* | all>
-output, -o	Especifica el formato de la salida. Sintaxis: -output format=<text | clpcsv | keyword | clpxml> O bien: -o format=<text | clpcsv | keyword | clpxml>
-version, -v	Muestra el número de versión de SM-CLP.

Navegación en el espacio de direcciones de MAP

NOTA: La barra diagonal (/) y la barra diagonal invertida (\) pueden intercambiarse en las rutas de acceso de direcciones en SM-CLP. Sin embargo, una barra 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 barra diagonal (/) o una barra diagonal invertida (\). Es el punto de partida predeterminado cuando se inicia sesión en el iDRAC6. Desplácese a la raíz con el verbo cd.

Por ejemplo, para navegar a la tercera anotación en el Registro de sucesos del sistema (SEL), introduzca el siguiente comando:

```
->cd /admin1/system1/logs1/log1/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 como funcionan en Windows y Linux: . . se refiere al nivel superior inmediato y . se refiere al nivel actual.

Destinos

Para consultar una lista de destinos disponibles a través de SM-CLP, consulte el documento de asignación de SM-CLP disponible en Dell Enterprise Technology Center en **www.delltechcenter.com**.

Uso del verbo show

Para conocer más sobre un destino, utilice el verbo show. Este verbo muestra las propiedades del destino, los subdestinos, asociaciones y una lista de 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, asociaciones y verbos. Por ejemplo, para mostrar sólo las propiedades y destinos en la ubicación actual, use el siguiente comando:

```
/admin1/system1/sp1/oemdcim_mfaaccount1 show -display properties,targets
```

Para mostrar sólo ciertas propiedades, indíquelas según se muestra en el siguiente comando:

```
show -d properties=(userid,name) /admin1/system1/sp1/oemdcim_mfaaccount1
```

Si sólo desea mostrar una propiedad, puede omitir los paréntesis.

Uso de la opción -level

La opción **show -level** ejecuta **show** en niveles adicionales debajo del del destino especificado. Para consultar todos los destinos y las propiedades en el espacio de direcciones, utilice la opción **-l all**:

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 (texto)** 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 (palabra clave)** muestra la información en forma de lista de pares palabra_clave=valor, un par por cada línea. El formato **clpxml** es un documento XML que contiene el elemento **response** XML (código XML de respuesta). El Grupo de trabajo de administración distribuida (DMTF) creó especificaciones para los formatos **clpcsv** y **clpxml**, que se encuentran en su sitio web en **www.dmtf.org**.

El siguiente ejemplo muestra cómo incluir el contenido del registro de sucesos del sistema en el mensaje de salida de XML:

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

Ejemplos de SM-CLP del iDRAC6

Las siguiente subsecciones ofrecen ejemplos sobre cómo iniciar sesión en el iDRAC6 mediante la interfaz SSH e iniciar una sesión SM-CLP para realizar las siguientes operaciones:

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

Administración de la alimentación del servidor

La Tabla 16-3 contiene ejemplos de cómo usar SM-CLP para realizar operaciones de administración de la alimentación del servidor en un servidor administrado.

Escriba "smclp" para iniciar la consola SM-CLP.

Tabla 16-3. 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: Escriba "smclp" para iniciar la consola SM-CLP.
Apagar el servidor	->stop /admin1/system1 system1 successfully stopped (detenido correctamente)
Encender el servidor a partir de un estado apagado	->start /admin1/system1 system1 successfully started (iniciado correctamente)
Reiniciar el servidor	->reset /admin1/system1 RESET successful for system 1 (RESTABLECIMIENTO correcto de system1)

Administración de SEL

La Tabla 16-4 contiene ejemplos de cómo usar SM-CLP para ejecutar operaciones relacionadas con SEL en el sistema administrado.

Navegación en MAP del destino

La

Tabla 16-4. Operaciones de administración del registro de sucesos del sistema

Operación	Sintaxis
Ver el SEL	->show -d targets,properties,verbs /admin1/system1/logs1/log1 **Podría informar lo siguiente:** Targets: record1/ record2/... Properties: OverwritePolicy=7 LogState=4 CurrentNumberOfRecords=60 MaxNumberOfRecords=512 ElementName=Record Log 1 HealthState=5 EnabledState=2 RequestedState=12 EnabledDefault=2 TransitioningToState=12 InstanceID=DCIM: SEL Log OperationalStatus={2} Verbs: show exit version cd help
Ver el registro de SEL	->show /admin1/system1/logs1/log1/record4 **Podría informar lo siguiente:** ufip=/admin1/system1/logs1/log1/record4 Associations:LogManagesRecord=>/admin1/system1/logs1/log1 Properties: RecordData=*0.0.65*4 2*1245152621*65 65*4*31*0*true*111*1*255*255* RecordFormat=*IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*IPMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI_GeneratorID*IPMI_EvMRev*I Description=:0:Assert:OEM specific ElementName=DCIM System Event Log Entry (Anotación del registro de sucesos del sistema DCIM) InstanceID=DCIM:SEL LOG:4 LogInstanceID=idrac:Unknown:Unknown SEL Log LogName=DCIM System Event Log Entry RecordID=DCIM:SEL LOG:4 CreationTimeStamp=20090616114341.000000+000
	Verbs: show exit version cd help delete
Borrar el SEL	->delete /admin1/system1/logs1/log1/record*

Informa:
Records deleted successfully (Registros eliminados correctamente).

Tabla 16-5 muestra ejemplos de cómo usar el verbo **cd** para navegar en MAP. En todos los ejemplos, se supone que el destino inicial predeterminado es /.

Tabla 16-5. Operaciones de navegación del mapa de destino

Operación	**Sintaxis**
Navegar hacia el sistema destino y reiniciar	->cd admin1/system1 ->reset **NOTA:** El destino predeterminado actual es **/**.
Navegar hacia el registro de sucesos del sistema (SEL) de destino y mostrar las anotaciones del registro	->cd admin1 ->cd system1 ->cd logs1 ->cd log1 ->show **es igual a** ->cd admin1/system1/logs1/log1 ->show
Mostrar el destino actual	->cd .
Subir un nivel	->cd ..
Salir del shell	->exit

Regresar a la página de contenido

Regresar a la página de contenido

Implementación del sistema operativo por medio de iVMCLI

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

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 Management Station al iDRAC6 en el sistema remoto. Por medio de la iVMCLI y los métodos con secuencias de comandos, es posible implementar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información acerca de cómo integrar la utilidad iVMCLI en su red de la empresa.

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 enumeran en las siguientes secciones.

Requisitos del sistema remoto

- El iDRAC6 se configura en cada sistema remoto.

Requisitos de red

Un recurso compartido de red debe tener los siguientes componentes:

- Los archivos del sistema operativo
- Los archivos controladores requeridos
- Los archivos de imagen de inicio del sistema operativo

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

Creación de un archivo de imagen de inicio

Antes de implementar el archivo de imagen en los sistemas remotos, compruebe que un sistema compatible pueda iniciar a partir del archivo. Para probar el archivo de imagen, transfiéralo a un sistema de prueba por medio de la interfaz web de usuario del iDRAC6 y reinicie el sistema.

Las siguientes secciones contienen información específica para la creación de archivos de imagen para sistemas Linux y Windows.

Creación de un archivo de imagen para sistemas Linux

Use la utilidad de duplicador de datos (dd) para crear un archivo de imagen de inicio para el sistema Linux.

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

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

Por ejemplo:

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

Creación de un archivo de imagen para sistemas Windows

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

Preparación para la implementación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que pueda acceder Management Station.
2. Copie los archivos del sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen de inicio preconfigurado para implementar el sistema operativo en los sistemas remotos, omita este paso.

   Si no tiene un archivo de imagen de inicio preconfigurado para implementación, prepárelo. Incluya los programas o secuencias de comandos que se van a utilizar para los procedimientos de implementación 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 implementación como "de sólo lectura" para garantizar que cada sistema de destino se inicie y ejecute el mismo procedimiento de implementación.

- Realice uno de los siguientes procedimientos:
  - Integre **IPMItool** y la interfaz de línea de comandos de medios virtuales (iVMCLI) en la aplicación existente de implementación 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 implementar el sistema operativo.

NOTA: **ivmdeploy** usa internamente **iVMCLI** y **ipmitool**. Para usar esta herramienta debe contar con privilegios para *IPMI en la LAN*. Asimismo, los medios virtuales deben estar en estado conectado cuando utilice la secuencia de comandos **ivmdeploy**.

Implementación del sistema operativo

Use la utilidad iVMCLI y la secuencia de comandos **ivmdeploy** que se incluye con la utilidad para implementar el sistema operativo en los sistemas remotos.

Antes de comenzar, repase 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 implementar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento ofrece una descripción de alto nivel para implementar 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 implementados en el archivo de texto **ip.txt**, una dirección IP por línea.
2. Inserte un CD o DVD de inicio 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 del 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 acerca de 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) se puede usar con secuencias de comandos y 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
- Finalización automática cuando la opción del firmware del iDRAC6 para iniciar una vez está activada
- Comunicaciones seguras con el iDRAC6 por medio de la capa de sockets seguros (SSL)

Antes de que ejecutar la utilidad, compruebe que cuenta con privilegios de usuario de medios virtuales en el iDRAC6.

PRECAUCIÓN: Se recomienda usar la opción '-i' de marcador interactivo al iniciar la utilidad de línea de comandos iVMCLI. Esto garantiza mayor seguridad al mantener en privado el nombre de usuario y la contraseña, ya que en muchos sistemas operativos Windows y Linux el nombre de usuario y la contraseña son visibles en formato de texto simple cuando los procesos son examinados por otros usuarios.

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 kit de software de administración de sistema Dell™ OpenManage™. 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 léame con la más reciente información de producto 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 implementar 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, copie 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_del_iDRAC>[:<puerto_SSL_del_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.

<*dirección_IP_de_iDRAC6*> es una dirección IP válida y única, o bien un 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 del iDRAC6.

Nombre de usuario del iDRAC6

`-u <nombre_de_usuario_del_iDRAC>`

Este parámetro proporciona el nombre de usuario del iDRAC6 que ejecutará los medios virtuales.

El <*nombre_de_usuario_del_iDRAC*> debe tener los atributos siguientes:

- Nombre de usuario válido
- Permiso de usuario de medios virtuales del 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 del iDRAC6 especificado.

Si la autentificación de iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Archivo de imagen o dispositivo de disco flexible / disco

`-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 disquete 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
soportes multimedia de CD/DVD. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Especifique al menos un tipo de medio (disco flexible o unidad de CD/DVD) con el comando, a menos que sólo se tengan opciones de interruptor. De lo contrario, aparecerá un mensaje de error y el comando terminará y producirá un error.

Mostrar la versión

-v

Este parámetro se usa para mostrar la versión de la utilidad 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 que se imprimieron 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 (&) 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 esta secuencia de comandos proceda después de iniciado 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 terminan manualmente, utilice las instalaciones específicas del sistema operativo para enumerar y terminar los 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

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

---

Descripción general

La utilidad de configuración del iDRAC6 es un entorno de configuración previo al inicio que permite ver y establecer parámetros para iDRAC6 y para el sistema administrado. Expresamente, usted puede:

- Ver los números de revisión del firmware del iDRAC6 y del firmware de de plano posterior primario.
- Configurar, activar o desactivar la red de área local (LAN) del iDRAC6
- Activar o desactivar la IPMI sobre LAN
- Configurar los parámetros de LAN
- Activar, desactivar o cancelar los servicios del sistema
- Activar o desactivar el descubrimiento automático y configurar el servidor de aprovisionamiento
- Conectar o desconectar los dispositivos de medios virtuales
- Activar o desactivar vFlash
- Activar o desactivar el inicio de sesión con tarjeta inteligente y el inicio de sesión único
- Configurar servicios del sistema
- Cambiar el nombre de usuario y la contraseña del administrador
- Restablecer la configuración predeterminada de fábrica del iDRAC6
- Ver o borrar 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 Dell™ OpenManage™, incluida la interfaz web, la interfaz de línea de comandos de SM-CLP, la interfaz de línea de comandos de RACADM local y remoto 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 **OSCAR (Configuración e informes en pantalla) del KVM** de iDRAC6. Use la <flecha hacia arriba> y <flecha hacia abajo> para resaltar la ranura que contiene el servidor y después oprima <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...`), oprima inmediatamente <Ctrl><E>. Aparece la utilidad de configuración del iDRAC6.

NOTA: Si el sistema operativo comienza a cargarse antes de que oprima <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 plano posterior primario. Los niveles de revisión pueden ser útiles para determinar si necesita actualizar el firmware.

El firmware del iDRAC6 es la parte del firmware que se encarga de las interfaces externas, por ejemplo, la interfaz web, SM-CLP y las interfaces web. El firmware de plano posterior primario es la parte del firmware que se conecta con el entorno de hardware del servidor y lo supervisa.

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 un elemento del menú conduce a un submenú o a un campo de texto editable, presione <Entrar> para acceder al elemento y <Esc> para salir de él después de terminar de configurarlo.
- 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 siguientes secciones describen las opciones del menú de la utilidad de configuración del iDRAC6.

LAN del 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 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 al iDRAC6 mediante 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 reciben cuando la LAN está desactivada. La interfaz RACADM local permanece disponible y se puede usar para reconfigurar la LAN del iDRAC6.

`Presione cualquier tecla para quitar el mensaje y continuar.`

IPMI en la LAN

Presione la tecla de flecha hacia la izquierda, la tecla de flecha hacia la derecha y la barra espaciadora para seleccionar entre **Activado** y **Desactivado**. Cuando se seleccione **Desactivado**, el iDRAC6 no aceptará mensajes IPMI que lleguen por medio de la interfaz de LAN.

Si elige **Desactivado**, aparecerá un mensaje de advertencia.

Presione cualquier tecla para quitar el mensaje y continuar. Para ver una explicación del mensaje, consulte "LAN del iDRAC6".

Parámetros de la LAN

Oprima <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 19-1. Parámetros de la LAN

Elemento	Descripción
Valores comunes	
Dirección MAC	Ésta es la dirección MAC no editable de la interfaz de red del iDRAC6.
Activar VLAN	Muestra **Activado**/**Desactivado**. **Activado** permitirá el filtrado de LAN virtual para el iDRAC6.
Identificación de VLAN	Muestra cualquier valor de identificación de VLAN entre 1 y 4094.
VLAN	Muestra la prioridad de la VLAN entre 0 y 7
Registrar el nombre del iDRAC6	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 iDRAC6	Si **Registrar el nombre del iDRAC** se encuentra **Activado**, presione <Entrar> para modificar el campo de texto **Nombre actual del iDRAC de DNS**. Presione <Entrar> cuando haya terminado de modificar el nombre del 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** está **Desactivado**, oprima <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`.
Cadena del nombre del host	Presione <Entrar> para editarla. Introduzca el nombre del host para alertas de captura de sucesos de plataforma (PET).
Alerta de LAN activada	Seleccione **Activado** para permitir un alerta de PET de LAN.
Entrada de política de alerta 1	Seleccione **Activar** o **Desactivar** para activar el primer destino de alerta.
Destino de alerta 1	Si **Alerta de LAN activada** está **Activada**, introduzca la dirección IP donde se enviarán las alertas de PET de LAN.
Configuración de IPv4	Active o desactive la compatibilidad para conexión IPv4.
IPv4	Seleccione **Activado** o **Desactivado** para la compatibilidad con el protocolo IPv4.

	El valor predeterminado es activado.
Clave de cifrado RMCP+	Presione <Entrar> para modificar el valor, <Esc> cuando haya terminado. La clave de cifrado 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.
Origen 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 **Origen de dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si la opción **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC6. La dirección predeterminada es **192.168.0.120.**
Máscara de subred	Si la opción **Origen de dirección IP** se establece como **DHCP**, este campo mostrará la dirección de máscara de subred que se obtuvo de DHCP. Si la opción **Origen de dirección IP** se establece como **Estática**, introduzca la máscara de subred para el iDRAC6. El valor predeterminado es **255.255.255.0**.
Puerta de enlace predeterminada	Si **Origen de dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada. El valor predeterminado es **192.168.0.1**.
Servidores DNS de DHCP	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidores DNS. Seleccione **Desactivado** para especificar las direcciones de servidores 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.
Configuración de IPv6	
IPv6	Active o desactive la compatibilidad para la conexión IPv6.
Origen de dirección IPv6	Seleccione entre **AutoConfig** y **Estática**. Cuando se selecciona **AutoConfig**, los campos **Dirección IPv6 1**, **Longitud del prefijo** y **Puerta de enlace predeterminada** se obtienen de DHCP. Cuando se selecciona **Estática**, las opciones **Dirección IPv6 1**, **Longitud del prefijo** y **Puerta de enlace predeterminada** se pueden editar.
Dirección IPv6 1	Si **Origen de dirección IP** se establece como **AutoConfig**, este campo mostrará la dirección IP que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC6.
Longitud del prefijo	Configura la longitud del prefijo de la dirección IPv6. Puede ser un valor entre 1 y 128, inclusive.
Puerta de enlace predeterminada	Si **Origen de dirección IP** se establece como **AutoConfig**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si **Origen de dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada.
Dirección IPv6 de vínculo local	Ésta es la **dirección IPv6 de vínculo local** no editable de la interfaz de red del iDRAC6.
Dirección IPv6 2-15	Ésta es la **dirección IPv6 2... dirección IPv6 15** no editable de la interfaz de red del iDRAC6.
Servidores DNS de DHCPv6	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidores DNS. Seleccione **Desactivado** para especificar las direcciones de servidores 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 primer servidor DNS.

Configuración de medios virtuales

Medios virtuales

Use la tecla de flecha hacia la izquierda y la tecla de flecha hacia la derecha para seleccionar las opciones **Conectado automáticamente**, **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**.
- Si selecciona la opción **Conectado automáticamente**, los dispositivos de medios virtuales se conectarán automáticamente con el servidor cuando se inicie una sesión de medios virtuales.

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 disquete en el sistema.

vFlash

Use la tecla de flecha hacia la izquierda y la tecla de flecha hacia la derecha para seleccionar **Activado** o **Desactivado**.

- **Activado**/**desactivado** hace que todos los dispositivos de medios virtuales del bus USB se **desconecten** y **conecten**.
- **Desactivado** hace que se elimine vFlash y ya no esté disponible para usar.

NOTA: Este campo puede ser de sólo lectura si una tarjeta SD con un tamaño superior a 256 MB no está presente en la ranura de la tarjeta Express del iDRAC6.

NOTA: Es necesario tener medios vFlash de la marca Dell para la partición de la unidad vFlash.

Tarjeta inteligente/SSO

Esta opción configura las funciones **Inicio de sesión de tarjeta inteligente** e **Inicio de sesión único**. Las opciones disponibles son **Activado** y **Desactivado**.

NOTA: Si activa la función **Inicio de sesión único**, se deshabilitará la función **Inicio de sesión de tarjeta inteligente**.

System Services

System Services

Use la tecla de flecha hacia la izquierda y la tecla de flecha hacia la derecha para seleccionar **Activado** o **Desactivado**. Si están activadas, algunas funciones de iDRAC6 pueden configurarse a través de Lifecycle Controller. Para obtener más información, consulte la *Guía del usuario de Lifecycle Controller,* disponible en el sitio web de asistencia de Dell en **support.dell.com/manuals**.

NOTA: Si modifica esta opción, el servidor se reiniciará cuando presione **Guardar** y **Salir** para aplicar la nueva configuración.

Cancelación de servicios del sistema

Use la tecla de flecha hacia arriba y la tecla de flecha hacia abajo para seleccionar **Sí** o **No**.

Al seleccionar **Sí**, se cierran todas las sesiones de Lifecycle Controller y el servidor se reinicia al presionar **Guardar** y **Salir** para aplicar la nueva configuración.

Recopilar el inventario del sistema en el reinicio

Seleccione la opción **Activado** para permitir la recopilación del inventario durante el reinicio. Para obtener más información, consulte la *Guía del usuario de Dell Lifecycle Controller*, disponible en el sitio web de asistencia de Dell: **support.dell.com/manuals**.

NOTA: Si esta opción se modifica, el servidor se reiniciará después de guardar la configuración y salir de la utilidad de configuración del iDRAC6.

Configuración de usuario de 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 LAN. Cuando haya terminado de configurar el usuario de LAN, presione <Esc> para volver al menú anterior.

Tabla 19-2. Pantalla de configuración de usuarios de la LAN

Elemento	Descripción
Descubrimiento automático	El descubrimiento automático permite descubrir automáticamente sistemas no aprovisionados en la red y establece *de manera segura* las credenciales iniciales para administrar estos sistemas. Esta función permite al iDRAC6 localizar el servidor de aprovisionamiento. El iDRAC6 y el servidor de servicio de aprovisionamiento se autentifican el uno al otro. El servidor de aprovisionamiento remoto envía las credenciales del usuario para que el iDRAC6 genere una cuenta de usuario con esas credenciales. Una vez creada la cuenta de usuario, una consola remota puede establecer una comunicación WSMAN con el iDRAC6 utilizando las credenciales especificadas en el proceso de descubrimiento y luego enviar instrucciones seguras al iDRAC6 para implementar un sistema operativo de manera remota. Para obtener información sobre la implementación remota del sistema operativo, consulte la *Guía del usuario de Dell Lifecycle Controller* disponible en el sitio web de asistencia de Dell: **support.dell.com/manuals**. Lleve a cabo los siguientes pasos previos en una sesión *independiente* de la **utilidad de configuración del iDRAC6** *antes de habilitar manualmente el descubrimiento automático*: - Activar NIC (servidores blade) - Activar IPv4 (servidores blade) - Activar DHCP - Obtener el nombre de dominio de DHCP - Deshabilitar la cuenta de administrador (cuenta n.º 2) - Obtener la dirección de servidor DNS desde DHCP - Obtener el nombre de dominio DNS de DHCP Seleccionar **Activado** para activar la función del descubrimiento automático. De manera predeterminada, la opción aparece como **desactivado**. Si solicitó un sistema Dell con la función del descubrimiento automático **Activado**, el iDRAC6 del sistema Dell se

	suministrará con DHCP activado sin credenciales predeterminadas para un inicio de sesión remoto.
Descubrimiento automático *(continuación)*	Antes de agregar el sistema Dell a la red y utilizar la función de descubrimiento automático, verifique los siguientes datos: • El servidor del protocolo de configuración dinámica de host (DHCP) y el sistema de nombres de dominio (DNS) están configurados. • Los servicios web de aprovisionamiento están instalados, configurados y registrados.
Servidor de aprovisionamiento	Este campo se utiliza para configurar el servidor de aprovisionamiento. La dirección del servidor puede ser una combinación de direcciones IPv4 o nombres de host y no debe superar los 255 caracteres. Cada dirección o nombre de host debe separarse por medio de una coma. Si activó la función de descubrimiento automático, las credenciales de usuario se obtienen del servidor de aprovisionamiento configurado para permitir el aprovisionamiento remoto en el futuro después de completar el proceso de descubrimiento automático correctamente. Para obtener más información, consulte la *Guía del usuario de Dell Lifecycle Controller* disponible en el sitio web de asistencia de Dell en **support.dell.com / manuals**.
Acceso a la cuenta	Seleccione **Activado** para activar la cuenta de administrador. Seleccione la opción **Desactivado** para desactivar la cuenta del administrador o en caso de que el descubrimiento automático está activado.
Privilegio LAN de IPMI	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? (Si restablece los valores predeterminados de fábrica restaurará la configuración no volátil de usuario remoto. ¿Continuar?)`

`< NO (NO) (Cancel (Cancelar)) >`

`< YES (SÍ) (Continue (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 entradas del registro y después muestra el número total de entradas y el mensaje más reciente. El SEL 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 web del iDRAC6.

Para borrar el SEL, seleccione **Borrar el registro de sucesos del sistema** y presione <Entrar>.

Cuando haya terminado con el menú del SEL, presione <Esc> para volver al menú anterior.

Cómo salir 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 de Managed System

Integrated Dell™ Remote Access Controller 6 (iDRAC6) Enterprise para servidores Blade versión 2.2 Guía del usuario

Esta sección explica cómo realizar las tareas relacionadas con los diagnósticos y solución de problemas de un sistema administrado remoto por medio de las utilidades del iDRAC6. Contiene las siguientes subsecciones:

- 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 podría enfrentar

---

La seguridad primero, para el usuario y para el sistema

Para realizar ciertos procedimientos de esta sección, debe trabajar con el chasis o con el sistema Dell PowerEdge™ o con otros módulos de hardware. No trate de reparar el hardware del sistema salvo cuando se explique en esta guía o en la documentación del sistema.

△ **PRECAUCIÓN: Muchas de las reparaciones sólo pueden realizarlas los técnicos de servicio autorizados. Sólo realice las soluciones de problemas y reparaciones sencillas autorizadas en la documentación del producto o según lo indique el equipo de servicio y asistencia técnica por teléfono o en línea. La garantía no cubre los daños ocasionados por reparaciones que Dell™ no ha autorizado. Lea y siga las instrucciones de seguridad incluidas 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 encontrar el componente que tiene la falla. Consulte la *Guía del usuario de firmware de Dell Chassis Management Controller* para obtener ayuda respecto del uso de la pantalla LCD.

La Tabla 20-1 describe el significado del comportamiento del indicador LED del sistema Dell PowerEdge:

Tabla 20-1. Indicadores LED del servidor blade

Indicador LED	Significado
verde continuo (*sólo para el botón de encendido*)	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, inspeccione el daño causado e intente corregir el problema con estas estrategias:

- Vuelva a insertar 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 para la solución de problemas del dispositivo de hardware.

Otros indicadores de problemas

Tabla 20-2. 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 del código de la POST del inicio	Consulte "Verificar los códigos de la 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 registro del 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 se tratan de solucionar de manera remota.

- Verificar la condición del sistema
- Consultar el registro de sucesos del sistema en busca de mensajes de error
- Consultar los códigos de la POST
- Visualización de la pantalla de último bloqueo
- Visualización de las secuencias de inicio más recientes
- Consulta de la pantalla de estado del servidor en la pantalla LCD en busca de mensajes de error
- Visualización del registro del iDRAC6
- Visualización de 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 pantalla **Resumen del sistema** muestra la condición de los componentes del sistema. La Tabla 20-3 describe el significado de los indicadores de condición del sistema.

Tabla 20-3. Indicadores de la condición del servidor

Indicador	Descripción
	Una marca de verificación verde indica una condición de estado satisfactoria (normal).
	Un triángulo amarillo que contiene un signo de exclamación 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 sección **Condición del servidor** 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 20-3), la fecha y hora, así como una descripción del suceso.
3. Haga clic en el botón **Registro de sucesos del sistema** correspondiente para continuar (consulte Tabla 20-4).

Tabla 20-4. 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 al usar Internet Explorer encuentra un problema al guardar, asegúrese de descargar la actualización de seguridad acumulada 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**.

Verificar los códigos de la POST

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

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

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

1. Haga clic en **Sistema**, luego en la ficha **Registros** y luego haga clic en **Código de la POST**.

   La pantalla **Código de la POST** muestra un indicador de condición del sistema (consulte la Tabla 20-3), un código hexadecimal y una descripción del código.
2. Haga clic en el botón **Código de la POST** correspondiente para continuar (consulte Tabla 20-5).

Tabla 20-5. Botones de Códigos de la POST

Botón	Acción
Imprimir	Imprime la **pantalla Código de la POST**.

Actualizar	Imprime la **pantalla Código de la 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 el almacén persistente 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 **Sistema**, luego en la ficha **Registros** y por último en **Pantalla de último bloqueo**.

La **Pantalla de último bloqueo** tiene los botones que se muestran en la Tabla 20-6:

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

Tabla 20-6. 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 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 en 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".

Visualización de las secuencias de inicio más recientes

Si experimenta problemas de inicio, puede ver la actividad de pantalla de lo sucedido durante las últimas tres secuencias de inicio desde la pantalla **Captura de inicio**. La reproducción de las pantallas de inicio ocurre a una velocidad de 1 marco por segundo. El iDRAC6 registra cincuenta marcos durante el tiempo de inicio.

La Tabla 20-7 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 20-7. Opciones de captura de inicio

Botón/Opción	Descripción
Selecciona la secuencia de inicio	Permite seleccionar la secuencia de inicio a cargar y reproducir. - Captura de inicio 1: Carga la secuencia de inicio más reciente. - Captura de inicio 2: Carga la (segunda) secuencia de inicio que ocurrió antes de la captura de inicio 1. - Captura de inicio 3: Carga la (tercera) secuencia de inicio 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 administrador 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.
Detener	Detiene la reproducción de pantalla y carga la primera pantalla de esa secuencia de inicio.
Pantalla siguiente	Lo lleva a la pantalla siguiente, de existir, en la consola de reproducción.
Imprimir	Imprime la imagen de la captura de inicio que aparece en la pantalla.
Actualizar	Vuelve a cargar la pantalla de la 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 20-8. Pantalla de estado del servidor

Gravedad	Mensaje	Causa
Advertencia	Temperatura ambiental de la placa del sistema: Sensor de temperatura de la placa del sistema, suceso de advertencia	La temperatura ambiental del servidor superó el umbral de advertencia
Crítico	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	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	Nivel de sistema de la placa del sistema: Sensor de corriente de la placa del sistema, suceso de advertencia	La corriente superó un umbral de advertencia
Crítico	Nivel de sistema de la placa del sistema: Sensor de corriente de la placa del sistema, suceso de falla	La corriente superó un umbral de falla
Crítico	CPU<número> <nombre del sensor de voltaje>:<número>sensor de voltaje de la CPU, se confirmó el estado declarado	Voltaje fuera de rango
Crítico	<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<número> <nombre del sensor de voltaje>:<número>sensor de voltaje de la CPU, se confirmó el estado declarado	Voltaje fuera de rango
Crítico	Estado de la CPU<número>: Sensor de procesador de la CPU<número>, se confirmó IERR	Falla de la CPU
Crítico	Estado de la CPU<número>: Sensor de procesador de la CPU<número>, se confirmó un disparo térmico	La CPU se sobrecalentó
Crítico	Estado de la CPU<número>: Sensor de procesador de la CPU<número>, se confirmó un error de configuración	Tipo incorrecto de procesador o instalación en el lugar erróneo
Crítico	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	Tarjeta elevadora 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	Estado de la tarjeta mezzanine B<número de ranura>: Sensor de tarjeta de complemento para la tarjeta mezzanine B<número de ranura>, se confirmó un error de instalación	Tarjeta mezzanine incorrecta instalada para la red Fabric de E/S
Crítico	Estado de la tarjeta mezzanine B<número de ranura>: Sensor de tarjeta de complemento para la tarjeta mezzanine B<número de ranura>, se confirmó un error de instalación	Tarjeta mezzanine incorrecta instalada para la red Fabric de E/S
Crítico	Unidad de plano posterior <número>: Sensor de ranura de unidad del plano posterior, se retiró la unidad	Se retiró la unidad de almacenamiento
Crítico	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	Protección contra fallas PFault de la placa del sistema: Sensor de voltaje de la placa del sistema, se confirmó el estado declarado	Este suceso se genera cuando los voltajes de la placa del sistema no se encuentran en los niveles normales
Crítico	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó que el temporizador expiró	El temporizador de vigilancia de iDRAC6 expiró y no se estableció ninguna acción
Crítico	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó un reinicio	La vigilancia de iDRAC6 detectó que el sistema se ha bloqueado (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de reiniciar
Crítico	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó el apagado	La vigilancia de iDRAC6 detectó que el sistema se ha bloqueado (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de apagado
Crítico	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó un ciclo de encendido	La vigilancia de iDRAC6 detectó que el sistema se ha bloqueado (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de ciclo de encendido
Crítico	Registro de sucesos de la placa del sistema: Sensor de registro de sucesos de la placa del sistema, se confirmó que el registro está lleno	El dispositivo de registro de sucesos del sistema detecta que sólo se podrá agregar una anotación al registro antes de que se llene
Advertencia	Error corregible ECC: Sensor de memoria, el ECC corregible (<ubicación del DIMM>) se confirmó	Los errores ECC corregibles alcanzaron una frecuencia crítica
Crítico	Error incorregible de ECC: un ECC incorregible (<ubicación del DIMM>) se confirmó	Se detectó un error ECC incorregible
Crítico	Rev. de canal de E/S: Sensor de sucesos críticos, se confirmó una NMI de revisión de canal de E/S	Se genera una interrupción crítica en el canal de E/S
Crítico	Error de paridad de PCI: Sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de paridad en el bus PCI
Crítico	Error de sistema de PCI: Sensor de sucesos críticos, se confirmó un SERR de PCI (<número de ranura o id. de dispositivo PCI>)	El dispositivo detectó un error de PCI
Crítico	Registro SBE desactivado: Sensor de registro de sucesos, se confirmó la desactivación del registro de errores corregibles de memoria	El registro de errores de un solo bit se desactiva cuando se registran demasiados SBE (errores de un solo bit)
Crítico	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	Error de protocolo de CPU: Sensor de procesador, se confirmó la transición a estado no recuperable	El protocolo del procesador ingresó a un estado no recuperable

No recuperable	PERR de bus de CPU: Sensor de procesador, se confirmó la transición a un estado no recuperable	El PERR de bus del procesador ingresó a un estado no recuperable
No recuperable	Error de inicialización de CPU: Sensor de procesador, se confirmó la transición a un estado no recuperable	La inicialización del procesador ingresó a un estado no recuperable
No recuperable	Revisión de máquina de CPU: Sensor de procesador, se confirmó la transición a un estado no recuperable	La revisión de máquina del procesador ingresó a un estado no recuperable
Crítico	Repuesto de memoria: Sensor de memoria, la pérdida de la redundancia (<ubicación del DIMM>) se confirmó	El repuesto de la memoria ya no es redundante
Crítico	Memoria reflejada: Sensor de memoria, la pérdida de la redundancia (<ubicación del DIMM>) se confirmó	La memoria reflejada ya no es redundante
Crítico	RAID de memoria: Sensor de memoria, la pérdida de la redundancia (<ubicación del DIMM>) se confirmó	La memoria de RAID ya no es redundante
Advertencia	Se agregó memoria: Sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>)	Se retiró el módulo de memoria agregado
Advertencia	Se quitó la memoria: Sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>)	Se retiró el módulo de memoria
Crítico	Error de configuración de memoria: Sensor de memoria, un error de configuración (<ubicación del DIMM>) se confirmó	La configuración de la memoria no es correcta para el sistema
Advertencia	Ganancia de redundancia de memoria: Sensor de memoria, la degradación de la redundancia (<ubicación del DIMM>) se confirmó	La redundancia de la memoria se ha degradado pero no se ha perdido
Crítico	Error fatal de PCIE: sensor de sucesos críticos, se confirmó un error fatal de bus	Se detectó un error fatal en el bus de PCIE
Crítico	Error de chipset: Sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de chip
Advertencia	Advertencia de 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	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	Error de la POST: Sensor de la POST, no hay memoria instalada	No se detectó memoria en la placa
Crítico	Error de la POST: Sensor de la POST, error de configuración de memoria	Se ha detectado la memoria, pero no se puede configurar
Crítico	Error de la POST: Sensor de la POST, error de memoria inutilizable	Se ha configurado la memoria, pero no se puede utilizar
Crítico	Error de la POST: Sensor de la POST, falló la caché rápida del BIOS	Falla de la caché rápida del BIOS del sistema
Crítico	Error de la POST: Sensor de la POST, falló el CMOS	Error de CMOS
Crítico	Error de la POST: Sensor de la POST, falló el DMA	Error del controlador DMA
Crítico	Error de la POST: Sensor de la POST, falló el controlador de interrupción	Falla del controlador de interrupción
Crítico	Error de la POST: Sensor de la POST, falló la actualización del temporizador	Error de actualización del temporizador
Crítico	Error de la POST: Sensor de la POST, error del temporizador de intervalos programable	Error del temporizador de intervalos programable
Crítico	Error de la POST: Sensor de la POST, error de paridad	Error de paridad
Crítico	Error de la POST: Sensor de la POST, falló el SIO	Error de SIO
Crítico	Error de la POST: Sensor de la POST, falló el controlador de teclado	Falla del controlador de teclado
Crítico	Error de la POST: Sensor de la POST, falló la inicialización de interrupción de administración del sistema	Falla de inicialización en la interrupción de administración del sistema
Crítico	Error de la POST: Sensor de la POST, falló la prueba de apagado del BIOS	Falla de la prueba de apagado del BIOS
Crítico	Error de la POST: Sensor de la POST, falló la prueba de apagado del BIOS	Falla de la prueba de la memoria del BIOS durante la POST
Crítico	Error de la POST: Sensor de la POST, falló la configuración de Dell Remote Access Controller	Falla de configuración de Dell Remote Access Controller
Crítico	Error de la POST: Sensor de la POST, falló la configuración de la CPU	Falla de configuración de la CPU
Crítico	Error de la POST: Sensor de la POST, configuración incorrecta de la memoria	Configuración incorrecta de la memoria
Crítico	Error de la POST: Sensor de la POST, falló la POST	Error general tras el vídeo
Crítico	Error de versión del hardware: Sensor de cambios de versión, se confirmó la incompatibilidad del hardware	Se detectó hardware incompatible
Crítico	Error de versión del hardware: Sensor de cambios de versión, se confirmó la incompatibilidad del hardware (firmware del BMC)	El hardware es incompatible con el firmware
Crítico	Error de versión del hardware: Sensor de cambios de versión, se confirmó la incompatibilidad del hardware (no hay correspondencia entre la CPU y el firmware del BMC)	La CPU y el firmware no son compatibles
Crítico	Sobrecalentamiento de memoria: Sensor de memoria, se confirmó un ECC corregible <ubicación del DIMM>	Sobrecalentamiento del módulo de memoria
Crítico	CRC fatal de SB de memoria: Sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Sur
Crítico	CRC fatal de NB de memoria: Sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Norte
Crítico	Temporizador de vigilancia: Sensor de vigilancia, se confirmó el reinicio	El temporizador de vigilancia hizo que el sistema se reiniciara
Crítico	Temporizador de vigilancia: Sensor de vigilancia, se confirmó la expiración del temporizador	El temporizador de vigilancia expiró pero no se realizó ninguna acción

Advertencia	Vínculo de asistencia: Sensor del cambio de la versión, no se declaró un cambio satisfactorio de software ni de firmware	No se pudo actualizar el valor del vínculo de asistencia para lograr un funcionamiento adecuado del NIC
Advertencia	Vínculo de asistencia: Sensor del cambio de la versión, no se declaró el cambio de hardware <número de ranura del dispositivo>	No se pudo actualizar el valor del vínculo de asistencia para lograr un funcionamiento adecuado del NIC
Crítico	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró el error de programación de la dirección MAC virtual (n.° de bus, n.° de dispositivo, n.° de función)	No se pudo programar FlexAddress para este dispositivo
Crítico	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró el error de la opción ROM del dispositivo para admitir el vínculo de asistencia o Flex Address (tarjeta mezzanine <ubicación>)	La opción ROM no admite ni FlexAddress ni el vínculo de asistencia
Crítico	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró el error en obtener datos del vínculo de asistencia o de FlexAddress del BMC/iDRAC6	Falló en obtener información del vínculo de asistencia o de FlexAddress del BMC/iDRAC6
Crítico	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró un error de la opción ROM del dispositivo para admitir el vínculo de asistencia o FlexAddress (tarjeta mezzanine XX)	Este suceso se genera si la opción ROM del dispositivo PCI de un NIC no admite el vínculo de asistencia o la función de direccionamiento de FlexAddress
Crítico	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró un error en la programación de la dirección MAC virtual (<ubicación>)	Este suceso se genera cuando el BIOS no puede programar la dirección MAC virtual en un NIC específico
Crítico	Error de E/S fatal: Sensor de grupo de E/S fatal, error fatal de E/S (<ubicación>)	Este suceso se genera en relación con un IERR de CPU e indica cuál de los dispositivos causó el IERR de CPU
Advertencia	Error de PCIE no fatal: Sensor de grupo E/S no fatal, error PCIe (<ubicación>)	Este suceso se genera en relación con un IERR de CPU

Visualización del registro del iDRAC6

El **registro** del iDRAC6 es un registro persistente que se mantiene en el firmware del iDRAC6. El registro contiene una lista de las acciones de usuario (como inicio, cierre de sesión y cambios de las políticas de seguridad) y de las alertas generadas por el iDRAC6. El registro se borra al actualizar el firmware del iDRAC6.

El **registro de sucesos del sistema** (SEL) contiene registros de sucesos que ocurren en el servidor administrado, mientras que el **registro** del iDRAC6 contiene registros de sucesos que ocurren en el iDRAC6.

Para acceder al **registro** del iDRAC6, realice los siguientes pasos:

- Haga clic en **Sistema**→ **Acceso remoto**→ **iDRAC6** y luego haga clic en **Registros** → **Registro del iDRAC6**.

El **registro del iDRAC6** proporciona la información de la Tabla 20-9.

Tabla 20-9. Información del registro del iDRAC6

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, 19 dic. 16:55:47). El iDRAC6 obtiene la hora del reloj del servidor administrado. Si el iDRAC6 se inicia y no se puede comunicar con el servidor administrado, la hora aparecerá como la cadena Inicio del sistema.
Origen	La interfaz que ocasionó el suceso.
Descripción	Una breve descripción del suceso y el nombre del usuario que inició sesión en el iDRAC6.

Uso de los botones de registro del iDRAC6

La pantalla **Registro** del iDRAC6 tiene los siguientes botones (consulte la Tabla 20-10).

Tabla 20-10. Botones del registro del iDRAC6

Botón	Acción
Imprimir	Imprime la pantalla **Registro** del iDRAC6.
Borrar registro	Borra las anotaciones del **Registro** del iDRAC6. **NOTA:** El botón **Borrar registro** sólo aparece si tiene permiso de **Borrar registros**.
Guardar como	Abre una ventana emergente que le permite guardar el **registro** del iDRAC6 en un directorio de su elección. **NOTA:** Si al usar Internet Explorer tiene un problema para guardar, asegúrese de descargar la actualización de seguridad acumulada 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 iDRAC6.

Ver la información del sistema

La pantalla **Resumen del sistema** muestra información sobre los siguientes componentes del sistema:

- Gabinete del sistema principal
- Integrated Dell Remote Access Controller 6: Enterprise

Para acceder a la información del sistema, haga clic en **Sistema→ Propiedades→ Detalles del sistema**.

Consulte "Recuperación y solución de problemas de Managed System" para obtener información sobre el resumen del sistema, el gabinete del sistema principal y el iDRAC6.

Identificación del servidor administrado en el chasis

El chasis Dell PowerEdge M1000e alberga hasta dieciséis servidores. Para localizar 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 de 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→ iDRAC6→ 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→ iDRAC6→ 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 20-11) que son similares a las herramientas que se incluyen con los sistemas con Microsoft® Windows® o Linux. Por medio de la interfaz web del 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→ iDRAC6→ Solución de problemas**.
2. Seleccione la ficha **Consola de diagnósticos**.

La Tabla 20-11 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 20-11. Comandos de diagnóstico

Comando	Descripción
arp	Muestra el contenido de la tabla del protocolo para resolución de direcciones (ARP). Las entradas 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.

ping6 <*dirección IPv6*>	Verifica que se pueda acceder a la dirección IPv6 de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se debe escribir una dirección IPv6 de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control en Internet) se envía a la dirección IPv6 de destino de acuerdo con el contenido de la tabla de enrutamiento actual.
traceroute <*dirección IP*>	Se usa para determinar la ruta que los paquetes toman en una red IP.
traceroute6 <*dirección IPv6*>	Se usa para determinar la ruta que los paquetes toman en una red IPv6.
gettracelog	Muestra el registro de rastreo del 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 del iDRAC6" para obtener ayuda con la configuración de permisos de usuario.

1. Haga clic en **Sistema** y luego en **Administración de la alimentación**→ ficha **Control de alimentación**.
2. Seleccione una **Operación de control de alimentación**, por ejemplo, **Restablecer el sistema (reinicio mediante sistema operativo)**. La Tabla 20-12 contiene información sobre las acciones de control de alimentación.
3. Haga clic en **Aplicar** para realizar la acción seleccionada.

Tabla 20-12. 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 apagar 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 (reinicio mediante suministro de energía)	Apaga el sistema y después lo reinicia (reinicio mediante suministro de energía).

Consulte "Supervisión y administración de alimentación" para obtener más información.

Solución de problemas y preguntas frecuentes

La Tabla 20-13 contiene la preguntas frecuentes sobre problemas de solución de problemas.

Tabla 20-13. Preguntas frecuentes/Solución de problemas

Pregunta	Respuesta
El indicador LED del servidor parpadea en color ámbar.	Verifique si hay mensajes en el SEL y borre el SEL 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 de SEL". En la utilidad de configuración del iDRAC6: • Consulte "Menú del registro de sucesos del sistema".

Hay un LED de color azul que parpadea 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 **Implementar**. 3. Lea la dirección IP del servidor en la tabla que aparece. **En el iKVM:** • Reinicie al servidor e ingrese a la **utilidad de configuración del iDRAC6** presionando <Ctrl><E>. • Espere la dirección IP que aparece durante la POST del BIOS. • Seleccione la consola "Dell CMC" consola en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos de RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *Guía de referencia del administrador de Dell Chassis Management Controller* para obtener una lista completa de los subcomandos de RACADM del CMC. • Use el comando **getsysinfo** de RACADM local para ver la dirección IP del iDRAC6.

	Por ejemplo:
	
	$ racadm getniccfg -m server-1
	
	DHCP activado = 1
	Dirección IP = 192.168.0.1
	Máscara de subred = 255.255.255.0
	Puerta de enlace = 192.168.0.1
	
	En RACADM local:
	
	Introduzca el comando siguiente en el símbolo del sistema:
	
	`racadm getsysinfo`
	
	En la pantalla LCD:
	
	1. En el menú principal, marque **Servidor** y oprima el botón de verificación.
	2. Seleccione el servidor de la dirección IP que busca y oprima 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** del CMC. **En el iKVM:** • Seleccione la consola "Dell CMC" consola en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos de RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *Guía de referencia del administrador de Dell Chassis Management Controller* para obtener una lista completa de los subcomandos de RACADM del CMC. $ racadm getniccfg -m chassis NIC activado = 1 DHCP activado = 1 Dirección IP estática = 192.168.0.120 Máscara de subred estática = 255.255.255.0 Puerta de enlace estática = 192.168.0.1 Dirección IP actual = 10.35.155.151 Máscara de subred actual = 255.255.255.0 Puerta de enlace actual = 10.35.155.1 Velocidad = Negociación automática Dúplex = Negociación automática **NOTA:** La acción anterior también puede realizarse mediante RACADM remoto.
La conexión de red del iDRAC6 no funciona.	• Asegúrese de que el cable de LAN esté conectado al CMC. • Asegúrese de que esté activada en el sistema la configuración de la NIC, la de IPv4 o IPv6, y que además esté activada la modalidad estática o DHCP.
Inserté el servidor en el chasis y presioné el botón de encendido, pero no pasó nada.	• El iDRAC6 requiere un máximo de 2 minutos para inicializarse antes de que el servidor se pueda encender. • 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 la configuración predeterminada del iDRAC6. 1. Reinicie el servidor y presione <Ctrl><E> cuando se le solicite para ingresar a la **utilidad de configuración del iDRAC6**. 2. En el menú **Utilidad de configuración del iDRAC6**, marque **Restablecer los valores predeterminados** y presione <Entrar>. **NOTA:** También puede restablecer el iDRAC6 desde RACADM local ejecutando `racadm racresetcfg`.

	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 inicia una sesión de redirección de consola en la interfaz web del iDRAC6, aparece una ventana emergente de seguridad de ActiveX.	iDRAC6 puede no ser un sitio de confianza. 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 en el explorador del cliente: 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 **Agregar**. 4. Haga clic en **Nivel personalizado**. 5. En la ventana **Configuración de seguridad**, seleccione **Petición** en **Descargar controles ActiveX no firmados**.
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 acceder a la función de medios virtuales, pero la consola del servidor administrado no aparecerá.
iDRAC6 no responde durante el inicio.	Retire el servidor e insértelo nuevamente. Revise la interfaz web del CMC para ver si el iDRAC6 aparece como un 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. - No hay tarjeta de vídeo 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