Dell Chassis Management Controller versión 3.10 para Dell EMC PowerEdge VRTX

Guía del usuario

DELL EMC

Notas, precauciónes y advertencias

NOTA: Una NOTA señala información importante que lo ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

ADVERTENCIA: Una señal de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

© 2013 - 2018 Dell Inc. o sus filiales. Todos los derechos reservados. Dell, EMC, y otras marcas comerciales son marcas comerciales de Dell Inc. o de sus subsidiarias. Otras marcas pueden ser marcas comerciales de sus respectivos propietarios.

2018 - 06

Rev. A01

Contenido

1

Resumen

Dell Chassis Management Controller (CMC) para Dell EMC PowerEdge VRTX es un hardware de administración de sistemas y una solución de software para administrar el chasis **PowerEdge VRTX**. La CMC cuenta con su propio microprocesador y memoria y recibe energía del chasis modular al que está conectado.

El CMC permite a un administrador de TI realizar lo siguiente:

- Ver el inventario
- Realizar tareas de configuración y supervisión
- Encender y apagar de forma remota el chasis y los servidores
- Activar alertas para los sucesos en los servidores y los componentes en el módulo del servidor
- Ver y administrar la controladora de almacenamiento y las unidades de disco duro en el chasis VRTX
- Administrar el subsistema PCIe en el chasis VRTX
- Proporcionar una interfaz de administración de uno a varios a los iDRAC y los módulos de E/S en el chasis

El chasis PowerEdge VRTX se puede configurar con una única CMC o con CMC redundantes. En las configuraciones de CMC redundante, si la CMC principal pierde la comunicación con el chasis o la red de administración, una CMC en espera asume la administración del chasis.

La CMC proporciona varias funciones de administración de sistemas para servidores. La administración térmica y de energía son las funciones principales de la CMC, las cuales se describen a continuación:

- Administración térmica y de energía automática en tiempo real de nivel de alojamiento.
  - La CMC supervisa los requisitos de energía del sistema y admite el modo opcional de Conexión dinámica de suministros de energía (DPSE). Este modo permite que la CMC mejore la eficiencia de energía al configurar los suministros de energía mientras el servidor está en modo de espera y administrar dinámicamente los requisitos de carga y redundancia.
  - El CMC informa el consumo de energía en tiempo real, lo que incluye el registro de los puntos máximos y mínimos con una indicación de hora.
  - El CMC admite la configuración de un límite opcional de energía máximo del gabinete (límite de energía de entrada del sistema), que envía alertas y realiza acciones como limitar el consumo de energía de los servidores y/o evitar encender nuevos servidores para mantener el gabinete dentro del límite de energía máximo definido.
  - El CMC supervisa y controla automáticamente las funciones de los ventiladores y sopladores en función de las mediciones de temperatura real ambiente e interna.
  - El CMC proporciona informes completos de errores o de estado y del inventario del gabinete.
- El CMC proporciona un mecanismo para configurar de forma centralizada lo siguiente:
  - Las configuraciones de red y seguridad del gabinete Dell PowerEdge VRTX
  - Los ajustes de redundancia de alimentación y de límite de energía.
  - Los ajustes de red de la iDRAC y los conmutadores de E/S
  - El primer dispositivo de inicio en el módulo del servidor
  - Verificaciones de consistencia de la red Fabric de E/S entre el módulo de E/S y los servidores. Asimismo, la CMC desactiva componentes, si es necesario, para proteger el hardware del sistema.
  - La seguridad de acceso de los usuarios.
  - Los componentes de almacenamiento, incluyendo el modo de tolerancia a errores para las controladoras de almacenamiento.
  - Las ranuras de PCIe

Es posible configurar el CMC para que envíe alertas por correo electrónico o alertas de las capturas SNMP por advertencias o errores como temperatura, configuración incorrecta del hardware, pérdida de energía, velocidad de los ventiladores y sopladores.

Temas:

Novedades de esta versión

Esta versión de la CMC para Dell EMC PowerEdge VRTX admite:

- Actualización del paquete de código abierto del kernel de Linux a la versión 4.9.31.
- Habilitación del protocolo de archivo compartido en Windows, versiones SMBv2 y SMBv3.
- Actualización del paquete OpenSSH de código abierto a la versión 7.6p1. La longitud mínima obligatoria de la clave de SSH es de 1024 bits.
- Compatibilidad con nombres de ranuras con una longitud de 24 caracteres para identificar a los servidores individuales.
- Activación de SNMP trap para la alerta TMP8501.
- Extensión de compatibilidad de la configuración de la dirección de fabric flex en el archivo **.xml** del perfil del chasis.
- Compatibilidad con identificadores de sesión de 128 bits.
- Funcionalidad de la criptografía 140-2 de los Federal Information Processing Standards (FIPS, Estándares de Procesamiento de la Información Federal).
- Actualización de firmware y controlador de tarjetas de comunicación en la 14. ª generación de servidores PowerEdge de Dell.

Funciones clave

Las funciones del CMC se agrupan en funciones de administración y de seguridad.

Funciones de administración

El CMC proporciona las siguientes funciones de administración:

- Entorno redundante del CMC.
- Registro del sistema dinámico de nombres de dominio (DDNS) para IPv4 e IPv6.
- Administración y configuración de inicio de sesión para usuarios locales, Active Directory y LDAP.
- Las opciones avanzadas de ventilación como ECM (Modo mejorado de ventilación) y desplazamiento de ventiladores se pueden activar para proporcionar ventilación adicional para un mejor rendimiento.
- Administración y supervisión remotas del sistema por medio de SNMP, una interfaz web, iKVM o una conexión de Telnet o SSH.
- Supervisión: proporciona acceso a la información del sistema y al estado de los componentes.
- Acceso a registros de sucesos del sistema: proporciona acceso al registro de hardware y al registro del chasis.

- Actualizaciones de firmware para diversos componentes del chasis: permite actualizar el firmware para CMC, iDRAC en los servidores, la infraestructura del chasis y el almacenamiento del chasis.
- Actualización de firmware para componentes del servidor, como el BIOS, las controladoras de red, las controladoras de almacenamiento, etc. en varios servidores del chasis con Lifecycle Controller.
- Integración con el software Dell OpenManage: permite iniciar la interfaz web del CMC desde Dell OpenManage Server Administrator u OpenManage Essentials (OME) 1.2.
- Alerta del CMC: alerta sobre problemas potenciales del nodo administrado mediante un mensaje por correo electrónico de syslog remoto o una captura SNMP.
- Administración remota de la alimentación: proporciona funciones remotas de administración de la alimentación, como el apagado y el restablecimiento de cualquier componente del chasis, desde una consola de administración.
- Informe de uso de la alimentación.
- Cifrado de capa de sockets seguros (SSL): ofrece administración remota y segura de sistemas mediante la interfaz web.
- Punto de inicio para la interfaz web de Integrated Dell Remote Access Controller (iDRAC).
- Compatibilidad con WS-Management.
- Función FlexAddress: reemplaza las direcciones WWN/MAC (Nombre a nivel mundial/Control de acceso a medios) asignadas de fábrica por direcciones WWN/MAC asignadas por el chasis para una ranura particular.
- Compatibilidad con la función de identidad de E/S de iDRAC para mejorar el inventario de direcciones WWN/MAC.
- Gráfico de la condición y el estado de los componentes del chasis.
- Asistencia para servidores simples o de varias ranuras.
- El asistente de configuración iDRAC con LCD admite la configuración de la red del iDRAC.
- Inicio de sesión único de iDRAC.
- Compatibilidad para el protocolo de hora de red (NTP).
- Resumen de servidores, informe de la alimentación y páginas de control de la alimentación mejorados.
- Protección forzada contra fallas del CMC y recolocación virtual de servidores.
- Administración de múltiples chasis donde se permite que hasta otros ocho chasis sean visibles desde el chasis principal.
- Configuración de componentes de almacenamiento en el chasis.
- Asignación de ranuras PCIe a los servidores y su identificación.

Funciones de seguridad

La CMC proporciona las siguientes funciones de seguridad:

- Administración de seguridad a nivel de contraseña: evita el acceso no autorizado a un sistema remoto.
- Autentificación centralizada de usuarios mediante:
  - Active Directory con esquema estándar o esquema extendido (opcional)
  - Identificaciones y contraseñas de usuarios guardadas en el hardware.
- Autoridad basada en funciones: permite que el administrador configure privilegios específicos para cada usuario.
- Configuración de identificaciones y contraseñas de usuario por medio de la interfaz web. La interfaz web admite cifrado SSL 3.0 de 128 bits y cifrado SSL 3.0 de 40 bits (para países en los que no se admiten 128 bits).

  NOTA: Telnet no admite el cifrado SSL.
- Puertos IP configurables (si corresponde).
- Límites de errores de inicio de sesión por dirección IP, con bloqueo de inicio de sesión proveniente de la dirección IP cuando esta última ha superado el límite.
- Límite de tiempo de espera de sesión automático y configurable, y varias sesiones simultáneas.
- Rango limitado de direcciones IP para clientes que se conectan a la CMC.
- Secure Shell (SSH), que utiliza una capa cifrada para ofrecer una mayor seguridad.
- Inicio de sesión único, autentificación de dos factores y autentificación de clave pública.

Descripción general del chasis

Esta figura muestra una vista de los conectores del CMC.

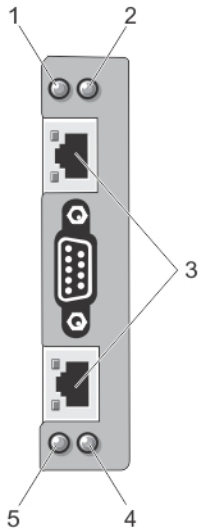


Figura 1. Conectores de la CMC y LED

Tabla 1. Conectores de la CMC y LED

Elemento	Indicador, botón o conector
1	Indicador de estado/identificación (CMC 1)
2	Indicador de alimentación (CMC 1)
3	Puertos del conector del CMC (2)
4	Indicador de alimentación (CMC 2)
5	Indicador de estado/identificación (CMC 2)

Aquí se proporciona una vista del panel posterior del chasis y una tabla que enumera las partes y los dispositivos disponibles en el CMC.

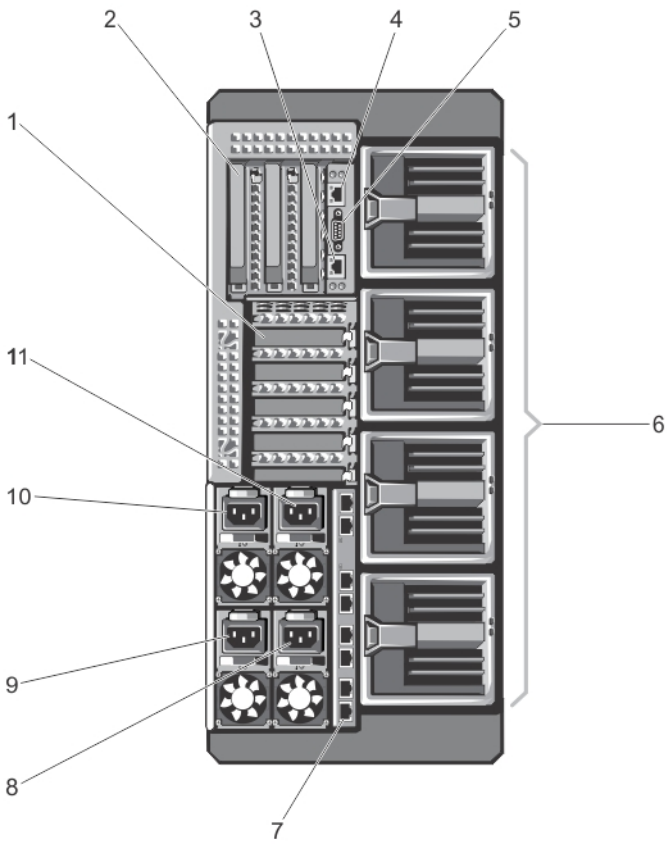


Figura 2. Panel posterior de la CMC

Tabla 2. Panel posterior de la CMC: piezas

Elemento	Indicador, botón o conector
1	Ranuras de tarjetas de expansión PCIe de perfil bajo (5)
2	Ranuras para tarjeta de expansión PCIe de altura completa (3)
3	Puerto GB Ethernet del CMC (CMC-2)
4	Puerto GB Ethernet del CMC (CMC-1)
5	Conector serie
6	Módulos de ventilación (4)
7	Puertos del módulo de E/S
8	PSU 4
9	PSU 3
10	PSU 1
11	PSU 2

Aquí se proporciona una vista del panel frontal del chasis y una tabla que enumera las partes y los dispositivos disponibles en el CMC.

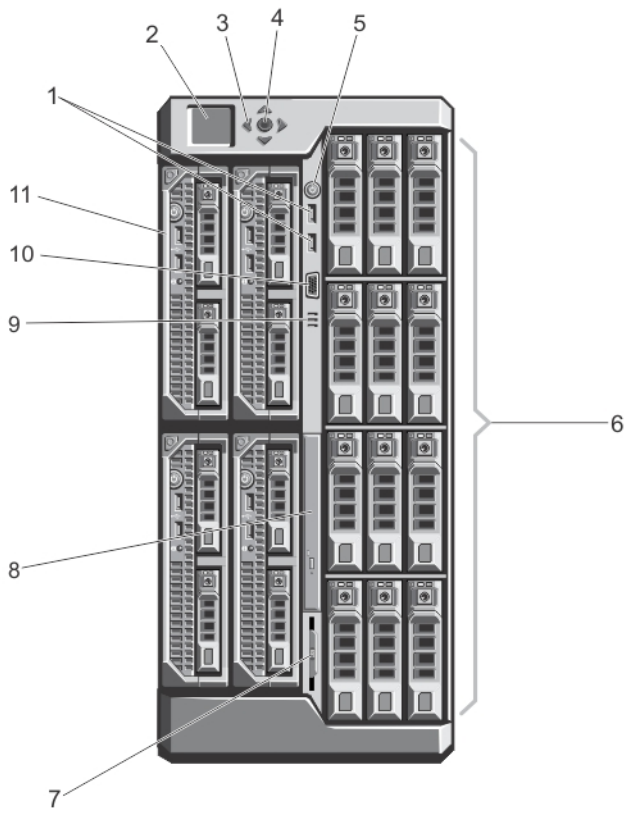


Figura 3. Características e indicadores del panel frontal: chasis de la unidad de disco duro de 3,5 pulgadas

Tabla 3. Características e indicadores del panel frontal

Elemento	Indicador, botón o conector	Descripción
1	Conectores USB (2)	Permite conectar un teclado y un mouse al sistema.
2	Panel LCD	Proporciona información sobre el sistema y su estado, así como mensajes de error para indicar que el sistema funciona correctamente o que se requiere atención.
3	Botones de desplazamiento del menú del LCD (4)	Desplaza el cursor en incrementos de un paso.
4	Botón de selección ("check")	Selecciona y guarda un elemento en la pantalla LCD y avanza a la pantalla siguiente.
5	Indicador de encendido, botón de encendido del gabinete	El indicador de encendido se ilumina cuando la alimentación del gabinete está activada. El botón de alimentación controla la salida de la PSU al sistema.
6	Unidades de disco duro	**Gabinete de unidades de disco duro de 2,5 pulgadas**: Hasta 25 unidades de disco duro de intercambio activo de 2,5 pulgadas. **Gabinete de unidades de disco duro de 3,5 pulgadas**: Hasta 12 unidades de disco duro de intercambio activo de 3,5 pulgadas.
7	Etiqueta de información	Panel de etiquetas de deslizamiento que permite registrar información del sistema, como la etiqueta de servicio, la NIC, la dirección MAC, la clasificación eléctrica del sistema y las marcas de las agencias reguladoras de todo el mundo.

Elemento	Indicador, botón o conector	Descripción
8	Unidad óptica (opcional)	Una unidad de DVD-ROM SATA o DVD+/-RW opcional.
9	Rejillas de ventilación	Rejillas de ventilación para el sensor de temperatura. **NOTA: Para asegurarse de que el enfriamiento sea adecuado, verifique que las rejillas de ventilación no estén bloqueadas.**
10	Conector de vídeo	Permite conectar un monitor al sistema.
11	Módulos del servidor	Hasta cuatro módulos de servidor PowerEdge M520, M620, M630 o M640, o bien, 2 módulos de servidor M820 específicamente configurados para el gabinete.

Versión mínima de CMC

En la siguiente tabla se incluye la versión mínima de CMC que se requiere para activar los módulos del servidor enumerados.

Tabla 4. Versión mínima de CMC para los módulos del servidor

Servidores	Versión mínima de CMC
PowerEdge M520	CMC 1.36
PowerEdge M620	CMC 1.36
PowerEdge M820	CMC 1.36
PowerEdge M630	CMC 2.00
PowerEdge M830	CMC 2.00
PowerEdge M640	CMC 3.00

En la siguiente tabla se incluye la versión mínima de CMC que se requiere para activar los módulos de E/S enumerados.

Tabla 5. Versión mínima de CMC para los módulos de E/S

Conmutadores de módulo de E/S	Versión mínima de CMC
Paso de 1 Gb R1 VRTX	CMC 1.20
Conmutador de R1-2401 VRTX de 1 GbE	CMC 1.20
Conmutador de 10 Gb R1-2210 VRTX	CMC 2.00

Conexiones de acceso remoto admitidas

En la siguiente tabla se muestran las conexiones de Remote Access Controller admitidas.

Tabla 6. Conexiones de acceso remoto admitidas

Conexión	Características
Puertos de la interfaz de red de la CMC	• Puerto GB: interfaz de red dedicada para la interfaz web del CMC • Compatibilidad con DHCP. • Notificación de sucesos por correo electrónico y capturas SNMP • Interfaz de red para el iDRAC y los módulos de E/S (IOM).

Conexión	Características
	• Compatibilidad con la consola de comandos Telnet/SSH y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado del sistema.
Puerto serie	• Compatibilidad con la consola serie y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado del sistema. • Compatibilidad con el intercambio binario para aplicaciones diseñadas para comunicarse mediante un protocolo binario con un tipo particular de módulo de E/S. • El puerto serie se puede conectar internamente a la consola serie de un servidor, o un módulo de E/S, mediante el comando connect (o racadm connect). • Proporciona acceso solamente al CMC activo

Plataformas admitidas

La CMC admite servidores modulares diseñados para la plataforma PowerEdge VRTX. Para obtener información sobre la compatibilidad con la CMC, consulte la documentación de su dispositivo.

Para obtener información sobre las plataformas más recientes, consulte *Dell Chassis Management Controller (CMC) Version 3.0 for Dell PowerEdge VRTX Release Notes* (Notas de publicación de Dell Chassis Management Controller (CMC) versión 1.00 para Dell PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Exploradores web compatibles

Dell PowerEdge VRTX admite los siguientes exploradores web:

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari versión 8.0.8
- Safari versión 9.0.3
- Mozilla Firefox 57
- Mozilla Firefox 58
- Google Chrome 62
- Google Chrome 63

NOTA: De manera predeterminada, TLS 1.1 y TLS 1.2 son compatibles con esta versión. Sin embargo, para activar TLS 1.0, utilice el siguiente comando racadm:

```
$ racadm config -g cfgRacTuning -o cfgRacTuneTLSProtocolVersionEnable TLSv1.0+
```

Administración de licencias

Las funciones de la CMC están disponibles según la licencia (CMC Express o CMC Enterprise) adquirida. Solo las funciones con licencia están disponibles en las interfaces que permiten configurar o usar la CMC. Por ejemplo, la interfaz web de la CMC, RACADM, WS-MAN, y así sucesivamente. La funcionalidad de administración y actualización del firmware de licencias de la CMC siempre está disponible a través de la interfaz web de la CMC y RACADM.

Tipos de licencias

A continuación se indican los tipos de licencias que se ofrecen:

- Evaluación de 30 días y extensión: la licencia vence después de 30 días y puede extenderse otros 30 días. Las licencias de evaluación se basan en períodos de tiempo y el cronómetro comienza a correr cuando se brinda alimentación al sistema.
- Perpetua: la licencia está enlazada a la etiqueta de servicio y es permanente.

Adquisición de licencias

Utilice cualquiera de los métodos siguientes para adquirir licencias:

- Correo electrónico: la licencia se adjunta a un correo electrónico que se envía después de solicitarlo del centro de asistencia técnica.
- Portal de autoservicio: en la CMC hay un vínculo al portal de autoservicio. Haga clic en él para abrir el Portal de autoservicio de licencias en Internet desde el que podrá adquirir licencias. Para obtener más información, consulte la ayuda en línea de la página del portal de autoservicio.
- Punto de venta: la licencia se adquiere al realizar un pedido de un sistema.

Operaciones de licencia

Antes de poder realizar las tareas de administración de licencias, asegúrese de adquirir las licencias. Para obtener más información, consulte la Guía de información general y funciones disponible en support.dell.com.

Puede realizar las siguientes operaciones de licencia mediante CMC, RACADM y WS-MAN para una administración de licencias de uno a uno y Dell License Manager para la administración de licencias de uno a varios:

NOTA: Si ha adquirido un sistema con todas las licencias previamente instaladas, no es necesario realizar tareas de administración de licencias.

- Ver: ver la información de la licencia actual.
- Importar: después de adquirir la licencia, guárdela en un almacenamiento local e impórtela en la CMC mediante una de las interfaces admitidas. La licencia se importa si supera todas las comprobaciones de validación.

  NOTA: Para algunas funciones, su activación requiere un reinicio del sistema.
- Exportar: exporte la licencia instalada en un dispositivo de almacenamiento externo como copia de seguridad o para reinstalarla después de reemplazar una parte de servicio. El nombre de archivo y formato de la licencia exportada es <EntitlementID>.xml
- Eliminar: elimine la licencia asignada a un componente cuando este no esté presente. Una vez eliminada la licencia, esta no se almacena en la CMC y se activarán las funciones del producto base.
- Reemplazar: reemplace la licencia para extender una licencia de evaluación, cambiar un tipo de licencia (tal como una licencia de evaluación por una licencia adquirida) o extender una licencia caducada.
- Una licencia de evaluación se puede reemplazar con una licencia de evaluación actualizada o con una licencia adquirida.
- Una licencia adquirida se puede reemplazar con una licencia actualizada o con una licencia ampliada. Para obtener más información acerca de la licencia, haga clic en Portal de administración de licencias de software de Dell.
- Más información: obtenga más información acerca de la licencia instalada o las licencias disponibles para un componente instalado en el servidor.

  NOTA: Para que la opción Más información muestre la página correcta, asegúrese de agregar *.dell.com a la lista de sitios de confianza en la configuración de seguridad. Para obtener más información, consulte la documentación de ayuda de Internet Explorer.

Estado o condición del componente de licencia y operaciones disponibles

En la tabla siguiente se proporciona la lista de operaciones de licencia disponibles en función del estado o la condición de la licencia.

Tabla 7. Operaciones de licencia según el estado y la condición

Estado o condición de la licencia o el componente	Import	Exportar	Eliminar	Reemplazar	Más información
Inicio de sesión no de administrador	No	Sí	No	No	Sí
Licencia activa	Sí	Sí	Sí	Sí	Sí
Licencia caducada	No	Sí	Sí	Sí	Sí
Licencia instalada pero falta el componente	No	Sí	Sí	No	Sí

Administración de licencias mediante la interfaz web del CMC

Para administrar licencias mediante la interfaz web del CMC, vaya a **Descripción general del chasis** > **Configuración** > **Licencias**.

Antes de importar una licencia, asegúrese de almacenar un archivo de licencia válido en el sistema local o en una red compartida a la que se pueda acceder desde CMC. La licencia está incorporada en un correo electrónico o se envía a través de este, desde el **Portal Web de autoservicio** o desde la herramienta de administración de claves de licencias.

La página **Licencias** muestra las licencias asociadas a los dispositivos o las licencias instaladas, pero el dispositivo no está presente en el sistema. Para obtener más información sobre la importación, exportación, eliminación o sustitución de licencias, consulte la *Ayuda en línea*.

Administración de licencias mediante RACADM

Para administrar licencias mediante los comandos RACADM, use el siguiente subcomando de licencia.

```
racadm license <license command type>
```

Para obtener más información acerca de los comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en dell.com/support/manuals.

Funciones con licencia en el CMC

La tabla contiene una lista de funciones del CMC que están activadas según su licencia.

Tabla 8. Funciones sujetas a licencia

Función	Express	Enterprise	Notas
Red de la CMC	Sí	Sí	
Puerto de serie de la CMC	Sí	Sí	
RACADM (SSH, local y remoto)	Sí	Sí	
Copia de seguridad de configuración del CMC	No	Sí	

Función	Express	Enterprise	Notas
Restauración de configuración del CMC	Sí	Sí	
WS-MAN	Sí	Sí	
SNMP	Sí	Sí	
Telnet	Sí	Sí	
SSH	Sí	Sí	
Interfaz basada en web	Sí	Sí	
Alertas de correo electrónico	Sí	Sí	
Implementación de LCD	Sí	Sí	
Administración extendida de iDRAC	Sí	Sí	
Syslog remoto	No	Sí	
Servicios de directorio	No*	Sí	*Para la configuración no predeterminada del servicio de directorio, Restablecer servicios de directorio solo se admite con una licencia Express. Restablecer servicios de directorio configurará los servicios de directorio a los valores predeterminados de fábrica.
Inicio de sesión único de iDRAC.	No	Sí	
Autentificación de dos factores	No	Sí	
Autenticación de PK	No	Sí	
Recurso compartido de archivos remotos	Sí	Sí	
Administración de recursos de ranura	No	Sí	
Límite de alimentación a nivel de gabinete	No*	Sí	*Para la configuración no predeterminada del límite de alimentación, Restaurar límite de alimentación solo se admite con una licencia Express. Restaurar límite de alimentación restablecerá el Límite de alimentación a los valores predeterminados de fábrica.
Conexión dinámica de suministros de energía	No*	Sí	*Para la configuración no predeterminada de DPSE, Restablecer DPSE solo se admite con una licencia Express. Restaurar DPSE restablecerá el DPSE a los valores predeterminados de fábrica.
Administración de chasis múltiples	No	Sí	
Configuración avanzada	No	Sí	
Copia de seguridad a nivel de gabinete	No	Sí	

Función	Express	Enterprise	Notas
Activación de FlexAddress	No*	Sí	*Para la configuración no predeterminada de FlexAddress, Restaurar valores predeterminados solo se admite con la licencia Express. Restaurar valores predeterminados restablecerá la dirección FlexAddress a los valores predeterminados de fábrica.
Asignación de adaptador de PCIe	Sí*	Sí	*Se puede asignar un máximo de dos adaptadores de PCIe por servidor con la licencia Express.
Adaptador virtual para la asignación de ranuras	No*	Sí	*Para la asignación no predeterminada de Adaptadores virtuales, Asignación predeterminada solo se admite con una licencia Express. Restaurar valores predeterminados cambiará la asignación del adaptador virtual a los valores predeterminados de fábrica.
Adaptador virtual para desasignación de ranuras	Sí	Sí	
Clonación de servidores	No	Sí	
Actualización de firmware del servidor de uno a muchos	No	Sí	
Configuración de uno a muchos para iDRAC	No	Sí	
Identidad de inicio	No	Sí	
Perfil del chasis	No	Sí	
Implementación rápida	No	Sí	

Visualización de versiones traducidas de la interfaz web del CMC

Para ver las versiones traducidas de la interfaz web del CMC, lea la documentación del explorador web.

Aplicaciones admitidas de la consola de administración

CMC admite la integración con la consola Dell OpenManage. Para obtener más información, consulte la documentación de la consola OpenManage disponible en **dell.com/support/manuals**.

Cómo usar esta guía

El contenido de esta guía del usuario permite realizar las tareas con:

- La interfaz web: aquí solo se proporciona información relacionada con las tareas. Para obtener información sobre los campos y las opciones, consulte *CMC for Dell PowerEdge VRTX Online Help (Ayuda en línea de la CMC para Dell PowerEdge VRTX)* que se puede abrir desde la interfaz web.
- Los comandos RACADM: aquí se proporciona el comando u objeto RACADM que debe usar. Para obtener más información acerca de un comando RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/cmcmanuals**.

Otros documentos que podrían ser de utilidad

Para acceder a los documentos desde el sitio de asistencia de Dell. Además de esta guía de referencia, puede acceder a las siguientes guías disponibles en **dell.com/support/manuals**.

- En *VRTX CMC Online Help (Ayuda en línea para la CMC de VRTX)*, se proporciona información sobre el uso de la interfaz web. Para acceder a la ayuda en línea, haga clic en **Ayuda** en la interfaz web del CMC.
- En *Chassis Management Controller Version 3.0 for Dell PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller versión 2.2 para Dell PowerEdge VRTX) se proporciona información sobre cómo usar las funciones RACADM relacionadas con VRTX.
- En *Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX Version 3.0 Release Notes* (Notas de publicación de Dell Chassis Management Controller (CMC) para Dell PowerEdge VRTX versión 2.20), disponibles en **dell.com/cmcmanuals**, se proporcionan actualizaciones de último minuto para el sistema, así como documentación o material de referencia con información técnica sobre opciones avanzadas para técnicos o usuarios experimentados.
- En *Integrated Dell Remote Access Controller (iDRAC) User's Guide* (Guía del usuario de Integrated Dell Remote Access Controller [iDRAC]), se ofrece información sobre la instalación, la configuración y el mantenimiento del iDRAC en sistemas administrados.
- La *Matriz de compatibilidad del subsistema de almacenamiento Dell PowerEdge VRTX* proporciona información sobre las versiones de referencia del subsistema de almacenamiento PowerEdge VRTX. Este documento está disponible en línea en **support.dell.com/manuals**.
- En *Dell OpenManage Server Administrator's User's Guide (Guía del usuario de Dell OpenManage Server Administrator)*, se proporciona información sobre la forma de instalar y utilizar Server Administrator.
- La *Guía de referencia de SNMP de Dell OpenManage para el iDRAC y Chassis Management Controller* proporciona información sobre los archivos MIB de SNMP.
- En *Dell Update Packages User's Guide (Guía del usuario de Dell Update Packages)*, se brinda información sobre la forma de obtener y usar Dell Update Packages como parte de la estrategia de actualización del sistema.
- La *Dell Shared PowerEdge RAID Controller (PERC) 8 User's Guide* (Guía del usuario de la Controladora Dell PowerEdge RAID (PERC) 8 compartida) proporciona información acerca de la implementación de la tarjeta PERC 8 compartida y la administración del subsistema de almacenamiento. Este documento está disponible en línea en **dell.com/storagecontrollermanuals**.
- En la documentación de la aplicación de administración de sistemas Dell se proporciona información sobre cómo instalar y utilizar el software de administración de sistemas.

La documentación del sistema siguiente proporciona más información sobre el sistema en el que está instalado el CMC de VRTX:

- Las instrucciones de seguridad incluidas con el sistema proporcionan información importante sobre la seguridad y las normativas. Para obtener más información sobre las normativas, consulte la página de inicio de cumplimento normativo en **www.dell.com/regulatory_compliance**. Es posible que se incluya información de garantía en este documento o en un documento separado.
- En *Dell PowerEdge VRTX Getting Started Guide* (Guía de introducción a Dell PowerEdge VRTX) que se envía con el sistema se ofrece una descripción general de las funciones del sistema, de la configuración del sistema y de las especificaciones técnicas.
- En el placemat de configuración que se envía con el sistema se ofrece información sobre la instalación y la configuración iniciales del sistema.
- En el *manual del propietario* del módulo del servidor se ofrece información acerca de las funciones del módulo del servidor y se describe cómo solucionar los problemas en el módulo del servidor e instalar o reemplazar los componentes del módulo del servidor. Este documento está disponible en línea en **dell.com/poweredgemanuals**.
- En la documentación del bastidor incluida con la solución del bastidor se describe cómo instalar el sistema en un bastidor, si es necesario.
- Para ver el nombre completo de las abreviaturas o siglas utilizadas en este documento, consulte Glossary (Glosario) en **dell.com/support/manuals**.
- En la documentación del software de administración de sistemas se describen las características, los requisitos, la instalación y el funcionamiento básico del software.
- En la documentación de los componentes adquiridos por separado se incluye información para configurar e instalar las opciones correspondientes.
- En el soporte suministrado con el sistema se incluye documentación y herramientas para configurar y administrar el sistema, incluidas las relacionadas con el sistema operativo, el software de administración del sistema, las actualizaciones del sistema y los componentes del sistema adquiridos con él. Para obtener más información sobre el sistema, explore el Localizador de recursos rápido (QRL) disponible en el sistema y en el placemat de configuración del sistema que se envía con el sistema. Descargue la aplicación QRL desde su plataforma móvil para habilitar la aplicación de su dispositivo móvil.

Acceso a documentos desde el sitio de asistencia de Dell EMC

Puede acceder a los documentos necesarios mediante una de las siguientes formas:

- Para ver documentos de Dell EMC Enterprise Systems Management: www.dell.com/SoftwareSecurityManuals
- Para ver documentos de Dell EMC OpenManage: www.dell.com/OpenManageManuals
- Para ver documentos de Dell EMC Remote Enterprise Systems Management: www.dell.com/esmmanuals
- Para ver documentos de iDRAC y Dell EMC Lifecycle Controller: www.dell.com/idracmanuals
- Para ver documentos de Dell EMC OpenManage Connections Enterprise Systems Management: www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Para ver documentos de Dell EMC Serviceability Tools: www.dell.com/ServiceabilityTools
- a Vaya a www.dell.com/Support/Home.

  b Haga clic en **Elegir entre todos los productos**.

  c En la sección **Todos los productos**, haga clic en **Software y seguridad** y, a continuación, haga clic en el vínculo necesario entre los siguientes:

  – **Administración de sistemas empresariales**
  – **Administración remota de sistemas empresariales**
  – **Herramientas de servicio**
  – **Conjunto de comandos del cliente de Dell**
  – **Administración de las conexiones de los sistemas del cliente**

  d Para ver un documento, haga clic en la versión del producto requerida.
- Mediante los motores de búsqueda:

  – Escriba el nombre y la versión del documento en el cuadro de búsqueda.

2

Instalación y configuración del CMC

En esta sección se proporciona información acerca de la forma de instalar el hardware del CMC, establecer el acceso al CMC, configurar el entorno de administración para utilizar el CMC, y usar los siguientes pasos como guía para configurar el CMC:

- Configurar el acceso inicial al CMC.
- Acceder al CMC a través de una red.
- Agregar y configurar usuarios del CMC.
- Actualización de firmware del CMC.

Para obtener más información sobre la instalación y la configuración de entornos de CMC redundantes, consulte Understanding Redundant CMC Environment (Descripción del entorno de CMC redundante).

Temas:

Antes de empezar

Antes de configurar el entorno del CMC, descargue la versión más reciente del firmware del CMC para PowerEdge VRTX en **dell.com/support/**.

Asimismo, asegúrese de que dispone del DVD *Dell Systems Management Tools and Documentation (Documentación y herramientas de administración de los sistemas Dell* que fue incluido con su sistema.

4Instalación de hardware del CMC

La CMC está preinstalada en el chasis, por lo que no se requiere su instalación. Es posible instalar una segunda CMC para que se ejecute como componente en espera para la CMC activa.

Lista de comprobación para configurar el chasis

Las siguientes tareas permiten configurar el chasis con precisión:

1 La CMC y la estación de administración, donde utiliza el explorador, deben estar en la misma red, la cual se denomina red de administración. Conecte un cable de red Ethernet del puerto activo de la CMC a la red de administración.

2 Instale el módulo de E/S en el chasis y conecte el cable de red al chasis.

3 Inserte los servidores en el chasis.

4 Conecte el chasis a la fuente de alimentación.

5 Presione el botón de encendido o encienda el chasis desde la interfaz web del CMC después de completar la tarea en el paso 7.

NOTA: No encienda los servidores.

6 Mediante el panel LCD, navegue hasta el resumen de IP y haga clic en el botón de selección "Verificar". Use la dirección IP de la CMC en el explorador del sistema de administración (E/S, Chrome o Mozilla). Para configurar DHCP para la CMC, use el panel LCD para hacer clic en **Menú principal** > **Configuración** > **Configuración de red**.

7 Conecte a la dirección IP del CMC mediante un explorador web al escribir el nombre de usuario predeterminado (root) y la contraseña (calvin).

8 Proporcione una dirección IP a cada iDRAC en la interfaz web del CMC y active la interfaz LAN e IPMI.

NOTA: La interfaz LAN del iDRAC está desactivada en algunos servidores de forma predeterminada. Esta información se puede encontrar en la interfaz web de la CMC en Descripción general del servidor > Configuración. Esta puede ser una opción de licencia avanzada, en cuyo caso se debe usar la función Configuración para cada servidor.

9 Proporcione al módulo de E/S una dirección IP en la interfaz web de la CMC. Es posible obtener la dirección IP al hacer clic en **Descripción general del módulo de E/S** y, a continuación, en **Configuración**.

10 Establezca conexión con cada iDRAC a través del explorador web y realice la configuración final del iDRAC. El nombre de usuario predeterminado es `root` y la contraseña es `calvin`.

11 Conecte el módulo de E/S mediante el explorador web y proporcione la configuración final del módulo de E/S.

12 Encienda los servidores e instale el sistema operativo.

NOTA: El CMC se reinicia si el panel de control se instala incorrectamente en el chasis.

Conexión básica del CMC a la red

Para obtener el grado más alto de redundancia, conecte cada CMC disponible a la red de administración.

Instalación de software de acceso remoto en una estación de administración

Es posible obtener acceso al CMC desde una estación de administración por medio de un software de acceso remoto, como las utilidades de consola Telnet, Secure Shell (SSH) o serie que se incluyen con el sistema operativo, o a través de la interfaz web.

Para utilizar el RACADM remoto desde la estación de administración, instale el RACADM remoto utilizando el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) que está disponible con el sistema. Este DVD incluye los siguientes componentes de Dell OpenManage:

- Directorio raíz del DVD: contiene Dell Systems Build and Update Utility.
- SYSMGMT: contiene productos de software de administración de sistemas, incluido Dell OpenManage Server Administrator.
- Docs: contiene documentación para sistemas, productos de software de administración de sistemas, periféricos y controladoras RAID.
- SERVICE: contiene las herramientas necesarias para configurar el sistema; además, proporciona los últimos diagnósticos y controladores optimizados por Dell para el sistema.

Para obtener más información sobre la instalación de los componentes de software de Dell OpenManage, consulte la *Dell OpenManage Installation and Security User's Guide (Guía del usuario de instalación y seguridad de Dell OpenManage)* disponible en el DVD o en **dell.com/support/manuals**. También puede descargar la última versión de las herramientas Dell DRAC Tools de **support.dell.com**.

Instalación de RACADM en una estación de administración con Linux

1 Inicie sesión como usuario raíz en el sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE Linux Enterprise Server admitido en el que desea instalar los componentes de Managed System.

2 Inserte el DVD *Dell Systems Management Tools and Documentation (Documentación y herramientas de Dell Systems Management)* en la unidad de DVD.

3 Para montar el DVD en una ubicación requerida, utilice el comando mount o un comando similar.

> **NOTA: En el sistema operativo Red Hat Enterprise Linux 5, los DVD se montan automáticamente mediante la opción. –noexec mount Esta opción no le permite iniciar ningún archivo ejecutable desde el DVD. Es necesario montar el DVD-ROM manualmente y, a continuación, ejecutar los comandos.**

4 Vaya al directorio **SYSMGMT/ManagementStation/linux/rac**. Para instalar el software RAC, escriba el siguiente comando:

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

5 Para obtener ayuda sobre el comando RACADM, escriba `racadm help` después de ejecutar los comandos anteriores. Para obtener más información acerca de RACADM, consulte *Chassis Management Controller for Dell PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM para Chassis Management Controller for Dell PowerEdge VRTX).

> **NOTA: Al utilizar la capacidad remota de RACADM, se debe tener permiso de escritura en las carpetas en las que se utilizan los subcomandos RACADM que involucran operaciones de archivos. Por ejemplo, `racadm getconfig -f <file name>`.**

Desinstalación de RACADM desde una estación de administración con Linux

1 Inicie sesión como `root` en el sistema en el que desea desinstalar las funciones de Management Station.

2 Use el siguiente comando de consulta rpm para determinar qué versión de DRAC Tools está instalada.

```
rpm -qa | grep mgmtst-racadm
```

3 Verifique la versión del paquete que desea desinstalar y desinstale la función mediante el comando `-e rpm -qa | grep mgmtst-racadm` de rpm.

Configuración de un explorador de web

Es posible configurar y administrar la CMC, los servidores y los módulos instalados en el chasis mediante un explorador web. Consulte la sección "Exploradores admitidos" en la *Dell System Software Support Matrix* (Matriz de compatibilidad de software de los sistemas Dell) en **dell.com/support/manuals**.

La CMC y la estación de administración, donde utiliza el explorador, deben estar en la misma red, la cual se denomina *red de administración*. En función de los requisitos de seguridad, la red de administración puede ser una red aislada y altamente segura.

> **NOTA: Asegúrese de que las medidas de seguridad en la red de administración, como los servidores de seguridad y los servidores proxy, no impidan que el explorador web obtenga acceso a la CMC.**

Algunas funciones de los exploradores pueden interferir con la conectividad o el rendimiento, especialmente si la red de administración no tiene una ruta a Internet. Si la estación de administración ejecuta un sistema operativo Windows, algunas configuraciones de Internet

Explorer pueden interferir con la conectividad, incluso cuando se utiliza una interfaz de línea de comandos para obtener acceso a la red de administración.

NOTA: Para solucionar problemas de seguridad, Microsoft Internet Explorer supervisa rigurosamente la hora en su administración de cookies. Para admitir esta función, la hora del equipo que ejecuta Internet Explorer debe estar sincronizada con la hora del CMC.

Servidor proxy

Para explorar a través de un servidor proxy que no posee acceso a la red de administración, es posible agregar las direcciones de la red de administración a la lista de excepciones del explorador. Esto indica al explorador que pase por alto el servidor proxy cuando intente obtener acceso a la red de administración.

Internet Explorer

Para editar la lista de excepciones en Internet Explorer:

1 Inicie Internet Explorer.
2 Haga clic en **Herramientas** > **Opciones de Internet** > **Conexiones**.
3 En la sección **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.
4 En la sección **Servidor proxy**, seleccione la opción **Utilizar un servidor proxy para la LAN (Esta configuración no se aplicará a las conexiones de marcación telefónica o VPN)** y, a continuación, haga clic en **Advanzada**.
5 En la sección **Excepciones**, agregue las direcciones para las CMC y las iDRAC de la red de administración a la lista de valores separados por punto y coma. Es posible usar nombres DNS y comodines en las entradas.

Mozilla Firefox

Para editar la lista de excepciones en Mozilla Firefox versión 19.0:

1 Abra Mozilla Firefox.
2 Haga clic en **Herramientas** > **Opciones** (para los sistemas que se ejecutan con), o bien, haga clic en **Editar** > **Preferencias**(para los sistemas que se ejecutan con Linux).
3 Haga clic en **Opciones avanzadas** y luego en la ficha **Red**.
4 Haga clic en **Configuración**.
5 Seleccione la opción **Configuración manual del proxy**.
6 En el campo **No usar proxy**, escriba las direcciones para las CMC y los iDRAC de la red de administración en la lista de valores separados por comas. Es posible usar nombres DNS y comodines en las anotaciones.

Filtro de suplantación de identidad de Microsoft

Si se activa el filtro de suplantación de identidad de Microsoft en el sistema de administración de Internet Explorer y la CMC no tiene acceso a Internet, el acceso a la CMC puede demorarse unos segundos. Esta demora puede ocurrir si se utiliza el explorador u otra interfaz como RACADM remoto. Para desactivar el filtro de suplantación de identidad:

1 Inicie Internet Explorer.
2 Haga clic en **Herramientas** > **Filtro de suplantación de identidad** y seleccione **Configuración del filtro de suplantación de identidad**.
3 Seleccione la opción **Desactivar el filtro de suplantación de identidad** y haga clic en **Aceptar**.

Obtención de la lista de revocación de certificados

Si la CMC no dispone de acceso a Internet, desactive la función de obtención de la lista de revocación de certificados (CRL) en Internet Explorer. Esta función prueba si un servidor, como el servidor web de la CMC, utiliza un certificado incluido en una lista de certificados revocados que se recupera de Internet. Si no es posible obtener acceso a Internet, esta función puede generar demoras de varios segundos cuando se obtiene acceso a la CMC mediante el explorador o con una interfaz de línea de comandos como el RACADM remoto.

Para desactivar la obtención de la CRL:

1 Inicie Internet Explorer.
2 Haga clic en **Herramientas** > **Opciones de Internet** y, a continuación, haga clic **Opciones avanzadas**.
3 Vaya a la sección Seguridad, desactive la opción **Comprobar si se revocó el certificado del editor** y haga clic en **Aceptar**.

Descarga de archivos desde el CMC con Internet Explorer

Cuando utiliza Internet Explorer para descargar archivos desde la CMC puede experimentar problemas cuando la opción **No guardar las páginas cifradas en el disco** está desactivada.

Para activar la opción **No guardar las páginas cifradas en el disco**:

1 Inicie Internet Explorer.
2 Haga clic en **Herramientas** > **Opciones de Internet** y, a continuación, haga clic en **Opciones avanzadas**.
3 En la sección **Seguridad**, seleccione la opción **No guardar las páginas cifradas en el disco**.

Activación de animaciones en Internet Explorer

Al transferir archivos hacia y desde la interfaz web, el ícono de transferencia de archivos gira para mostrar la actividad de transferencia. Si utiliza Internet Explorer, debe configurar el explorador para reproducir animaciones.

Para configurar Internet Explorer para reproducir animaciones:

1 Inicie Internet Explorer.
2 Haga clic en **Herramientas** > **Opciones de Internet** y, a continuación, haga clic en **Opciones avanzadas**.
3 Vaya a la sección **Multimedia** y seleccione la opción **Activar animaciones en páginas web**.

Configuración del acceso inicial al CMC

Para administrar el CMC de manera remota, conecte el CMC a la red de administración y luego establezca la configuración de red del CMC.

NOTA: Para administrar M1000e, esa solución debe estar conectada a la red de administración.

Para obtener más información sobre la configuración de los valores de red de la CMC, consulte Configuración inicial de la red de la CMC. Esta configuración inicial asigna los parámetros de red TCP/IP que permiten obtener acceso a la CMC.

La CMC y el iDRAC en cada servidor, y los puertos de administración de red del módulo de E/S del conmutador se conectan a una red integrada común en el chasis PowerEdge VRTX. Esto permite aislar la red de administración de la red de datos de servidores. Es importante separar el tráfico para garantizar el acceso ininterrumpido a las funciones de administración del chasis.

La CMC se conecta a la red de administración. Todo acceso externo a la CMC y a los iDRAC se realiza mediante la CMC. Por otro lado, el acceso a los servidores administrados se realiza mediante conexiones de red al módulo de E/S (IOM). Esto permite aislar la red de aplicaciones de la red de administración.

Se recomienda aislar la administración del chasis de la red de datos. Debido a la posibilidad de que exista tráfico en la red de datos, las interfaces de administración en la red de administración interna se pueden saturar con el tráfico dirigido a los servidores. Esto ocasiona demoras en la comunicación entre la CMC y el iDRAC. Estas demoras pueden provocar un comportamiento impredecible en el chasis, como por ejemplo, que la CMC muestre el iDRAC sin conexión, aunque esté encendido y en funcionamiento, lo que a su vez genera otros comportamientos no deseados. Si no es práctico aislar físicamente la red de administración, la otra opción es enviar el tráfico de la CMC y del iDRAC a una red VLAN separada. Las interfaces de red del iDRAC individual y de la CMC pueden configurarse para usar una red VLAN.

Configuración inicial de red del CMC

NOTA: Al cambiar la configuración de red del CMC, es posible que la conexión de red actual se desconecte.

Puede realizar la configuración inicial de red de la CMC antes o después de que la CMC tenga una dirección IP. Si configura las opciones iniciales de red iniciales antes de tener una dirección IP, puede utilizar cualquiera de las siguientes interfaces:

- El panel LCD en el frente del chasis
- La consola serie del CMC de Dell

Si se establece la configuración inicial de red después de asignar una dirección IP al CMC, se puede utilizar cualquiera de las siguientes interfaces:

- Interfaces de línea de comandos (CLI), como una consola serie, Telnet, SSH o Dell CMC Console
- RACADM remoto
- Interfaz web del CMC
- Interfaz del panel LCD

La CMC admite los modos de direccionamiento IPv4 e IPv6. Los valores de configuración para IPv4 e IPv6 son independientes entre sí.

Configuración de la red del CMC mediante la interfaz del panel LCD

El panel LCD puede utilizarse para configurar la interfaz de red del CMC.

NOTA: Puede personalizar la orientación de una pantalla LCD (para bastidor o modo torre) manteniendo los botones arriba y abajo presionados durante dos segundos. De manera alternativa, también puede utilizar los botones derecho e izquierdo. Para obtener más información sobre los botones que están disponibles en un panel LCD de la CMC, consulte Navegación por la pantalla LCD.

1 Para iniciar la configuración del CMC:
   - En el caso de un chasis que no se haya configurado anteriormente, aparecerá el panel **Idioma de LCD**. En el panel **Idioma de LCD**, elija el idioma requerido mediante el uso de los botones de flecha. Cuando se resalta el idioma deseado, para seleccionar el idioma, presione el botón del centro. Aparecerá el panel **Configuración de la red**.
   - En el caso de un chasis que se haya configurado anteriormente, aparecerá el panel **Menú principal**. Desde el **Menú principal**, seleccione **Configuración** y, a continuación, **Configuración de red**.

2 En el panel **Configuración de red**, seleccione el modo de configuración requerido:
   - **Configuración rápida (DHCP)**: seleccione este modo para configurar la CMC rápidamente mediante las direcciones de DHCP. Para obtener información sobre la configuración de la CMC a través de este modo, consulte **Configuración de la CMC mediante la herramienta de configuración rápida (DHCP)**.
   - **Configuración avanzada**: seleccione este modo para establecer la configuración avanzada de la CMC. Para obtener información sobre la configuración de la CMC utilizando este modo, consulte **Configuración de la CMC mediante la herramienta de configuración avanzada**.

Configuración del CMC mediante la herramienta de configuración rápida (DHCP)

Para configurar una red mediante la interfaz del panel LCD:

1 En el panel **Configuración de red**, seleccione **Configuración rápida (DHCP)**. El panel muestra el siguiente mensaje.

```
About to get DHCP addresses. Ensure CMC network cable is connected.
```

2 Presione el botón central para resaltar el botón aceptar. Presione el botón central nuevamente para confirmar la configuración o desplácese hasta la flecha posterior y presione el botón central para regresar y modificar la configuración.

Configuración avanzada del CMC

1 En el panel **Configuración de red**, si selecciona **Configuración avanzada**, se muestra el siguiente mensaje para confirmar si desea configurar el CMC:

```
Configure CMC?
```

2 Para configurar el CMC mediante el uso de las propiedades de configuración avanzada, haga clic en el botón central seleccionando el icono de verificación.

> **NOTA: Para omitir la configuración del CMC, vaya al icono 'X' y presione el botón central.**

3 Si el sistema le solicita que seleccione una velocidad de la red adecuada, seleccione una velocidad de la red (**Negociación automática (1 Gb)**,**10 Mb** o **100 Mb**) con los botones correspondientes.

Para lograr un rendimiento efectivo de la red, el valor de velocidad de la red debe coincidir con la configuración de la red. Un valor de velocidad de la red inferior a la velocidad en la configuración de la red aumenta el consumo de ancho de banda y reduce la velocidad de la comunicación de red. Es necesario determinar si la red admite las velocidades de red anteriores y definir los valores según corresponda. Si la configuración de la red no coincide con alguno de estos valores, se recomienda seleccionar la opción **Automático (1 GB)** o consultar al fabricante de los equipos de red.

4 Realice una de las siguientes tareas:

- Seleccione **Automático (1 Gb)** pulsando el botón central y, a continuación, presione el botón central nuevamente. Aparece el panel **Protocolo**. Vaya al paso 6.
- Seleccione **10 Mb** o **100 Mb**. El panel **Dúplex**

  se muestre. Vaya al paso 5.

De lo contrario, si usted

5 En el panel **Dúplex**, para seleccionar el modo dúplex (**Total** o **Medio**) que coincide con el entorno de red, presione el botón central y, a continuación, vuelva a presionar el mismo botón. Aparece el panel **Protocolo**.

> **NOTA: La configuración de la velocidad de la red y de modo dúplex no estará disponible si Negociación automática se establece como Activada o si se selecciona 1000 MB (1 Gbps). Si la Negociación automática está activada para un dispositivo pero no para el otro, el dispositivo que utiliza Negociación automática puede determinar la velocidad de la red del otro dispositivo, pero no el Modo dúplex. En este caso, se selecciona medio dúplex como el modo dúplex durante la negociación automática. Una incompatibilidad de dúplex de este tipo genera una conexión de red lenta.**

6 En el panel **Protocolo**, seleccione el protocolo de Internet (**Solo IPv4**, **Solo IPv6** o **Ambos**) que desea utilizar para el CMC, presione el botón central y, a continuación, vuelva a presionar el mismo botón.

7
- Si selecciona **IPv4** o **Ambos**, seleccione modo **DHCP** o **Estático**. Vaya al paso 8.
- De lo contrario, si selecciona **IPv6**, aparecerá el panel **Configurar iDRAC**. Vaya al paso 11 más adelante en este procedimiento.

8 En el panel **Modo**, seleccione el modo en el que la CMC obtendrá las direcciones IP de NIC. Si selecciona DHCP, la CMC recupera automáticamente la configuración de IP (dirección IP, máscara y puerta de enlace) de un servidor DHCP en la red. A la CMC se le asigna una dirección IP única que se distribuye en la red. Si selecciona **DHCP**, presione el botón central y, a continuación, vuelva a presionar el mismo botón. Aparecerá el panel **Configurar iDRAC**. Vaya al paso 11 más adelante en este procedimiento.

9 Si selecciona **Estática**, introduzca la dirección IP, la puerta de enlace y la máscara de subred de acuerdo con las instrucciones en el panel LCD.

Se muestra la información IP que introdujo. Presione el botón central y, a continuación, vuelva a presionar el mismo botón. La pantalla **Configuración de la CMC** enumera los valores de **Dirección IP estática**, **Máscara de subred**) y **Puerta de enlace** que haya especificado. Compruebe la configuración para asegurarse de su precisión. Para corregir un valor, presione los botones correspondientes. Presione el botón central y, a continuación, vuelva a presionar el mismo botón. Aparecerá el panel **¿Registrar DNS?** .

10 Para registrarlo, seleccione el ícono de verificación y luego, presione el botón central. Establezca la dirección IP de DNS, seleccione el ícono de verificación y, a continuación, presione el botón central. Si el registro de DNS no es necesario, seleccione el ícono 'X' y presione el botón central.

11 Indique si desea o no configurar iDRAC:

- **No**: seleccione el ícono 'X' y, a continuación, presione el botón central. Vaya al paso 17 más adelante en este procedimiento.
- **Sí**: seleccione el icono de verificación y, a continuación, presione el botón central.

También puede configurar iDRAC desde la interfaz web del CMC.

12 En el panel **Protocolo**, seleccione el tipo de IP que desea usar para los servidores:

- **IPv4**: se muestran las opciones **DHCP** o **Estática**.
- **Ambos**

  : se muestran las opciones de **DHCP** o **Estática**.
- **IPv6**

  — Aparece el panel **Configuración del iDRAC**. Vaya al paso 15.

13 Seleccione **DHCP** o **Estática**.

Tabla 9. Modo de red

Protocolo de configuración dinámica de host (DHCP)	iDRAC recupera automáticamente la configuración de IP (dirección IP, máscara y puerta de enlace) de un servidor DHCP en la red. Al iDRAC se le asigna una dirección IP única a través de la red. Presione el botón central. Aparece el panel **IPMI en la LAN**.

Estática	Si selecciona **Estática**, introduzca manualmente la dirección IP, la puerta de enlace y la máscara de subred de acuerdo con las instrucciones en la pantalla LCD.
	Si ha seleccionado la opción **Estática**, presione el botón central y, a continuación, haga lo siguiente:
	a El siguiente mensaje le pregunta si desea o no incrementar de forma automática mediante la IP de ranura-1.
	`IPs will auto-increment by slot number.`
	Haga clic en el botón central. El siguiente mensaje le solicita que introduzca el número de IP de la ranura-1.
	`Enter slot 1 (starting) IP`
	Introduzca el número de IP de la ranura-1 y luego presione el botón central.
	b Introduzca el número de IP de la ranura-1 y, a continuación, presione el botón central.
	c Establezca la puerta de enlace y, a continuación, presione el botón central.
	d La pantalla **Resumen de red** muestra los valores de **Dirección IP estática**, **Máscara de subred** y **Puerta de enlace** que haya especificado. Compruebe la configuración para asegurarse de su precisión. Para corregir un valor, presione los botones correspondientes y, a continuación, presione el botón central.
	e Cuando haya confirmado la precisión de la configuración introducida, vaya al paso 10.
	Aparece el panel **IPMI en la LAN**.

14 En el panel **IPMI en la LAN**, seleccione **Activar** o **Desactivar** para activar o desactivar la IPMI en la LAN. Presione el botón central para continuar.

15 En el panel **Configuración de iDRAC** se muestra el siguiente mensaje.

```
Apply settings to installed servers?
```

Para aplicar toda la configuración de red del iDRAC a los servidores instalados, seleccione el ícono de verificación y, a continuación, presione el botón central. De lo contrario, seleccione el ícono 'X' y, a continuación, presione el botón central.

16 En el panel **Configuración de iDRAC** se muestra el siguiente mensaje.

```
Auto-Apply settings to newly-inserted servers?
```

Para aplicar toda la configuración de red del iDRAC a los servidores recientemente instalados, seleccione el ícono de verificación y, a continuación, presione el botón central. Cuando se inserta un nuevo servidor en el chasis, el LCD le solicita si desea implementar automáticamente el servidor con las políticas de configuración de red establecidas anteriormente. Si no desea aplicar la configuración de red del iDRAC a los servidores recientemente instalados, seleccione el ícono 'X' y presione el botón central. Cuando se inserta un nuevo servidor en el chasis, no se configuran los valores de la red de iDRAC.

17 En el panel **Configuración de iDRAC** se muestra el siguiente mensaje.

```
Apply All Enclosure Settings?
```

Para aplicar toda la configuración del gabinete, seleccione el ícono de verificación y presione el botón central. De lo contrario, seleccione el ícono 'X' y, a continuación, presione el botón central.

18 En el panel **Resumen de IP**, después del panel de espera de 30 segundos, revise las direcciones IP suministradas para asegurarse de que sean las correctas. Para corregir un valor, presione el ícono de flecha izquierda y luego presione la tecla central para regresar a la pantalla correspondiente a ese valor. Después de corregir una dirección IP, presione el botón central.

Cuando haya confirmado la precisión de los valores introducidos, presione el botón central y, a continuación, vuelva a presionar el mismo botón. Aparecerá la ID del panel **Menú principal**.

La CMC y los iDRAC ahora están disponibles en la red. Puede obtener acceso a la CMC en la dirección IP asignada por medio de la interfaz web o las CLI, como por ejemplo, una consola serie, Telnet y SSH.

Interfaces y protocolos para obtener acceso al CMC

Una vez configurados los valores de red de la CMC, es posible obtener acceso a la CMC de manera remota por medio de diversas interfaces. En la siguiente tabla se enumeran las interfaces que se pueden utilizar para obtener acceso a la CMC de manera remota.

NOTA: Debido a que Telnet no ofrece tanta seguridad como las otras interfaces, esa opción está desactivada de manera predeterminada. Active Telnet mediante la web, SSH o el RACADM remoto.

NOTA: Si se utiliza más de una interfaz al mismo tiempo, se pueden obtener resultados inesperados.

Tabla 10. Interfaces del CMC

Interfaz	Descripción
Interfaz web	Proporciona acceso remoto a la CMC mediante una interfaz gráfica de usuario. La interfaz web está incorporada en el firmware de la CMC y se puede acceder por medio de la interfaz del NIC desde un explorador web compatible en la estación de administración. Para obtener una lista de los exploradores web compatibles, consulte la sección correspondiente en *Dell System Software Support Matrix* (Matriz de compatibilidad de software de los sistemas Dell) en **dell.com/support/manuals**.
Interfaz de línea de comandos de RACADM remoto	Use esta utilidad de línea de comandos para administrar el CMC y sus componentes. Puede usar el RACADM de firmware o el RACADM remoto: • El RACADM remoto es una utilidad cliente que se ejecuta en una estación de administración. Utiliza la interfaz de red fuera de banda para ejecutar los comandos de RACADM en los sistemas administrados y el canal HTTPS. La opción `–r` ejecuta el comando RACADM a través de una red. • El RACADM de firmware no es accesible al iniciar sesión en la CMC mediante SSH o Telnet. Puede ejecutar los comandos de RACADM de firmware sin especificar la dirección IP de la CMC, el nombre de usuario o la contraseña. Después de entrar en el símbolo del sistema de RACADM, puede ejecutar directamente los comandos sin el prefijo racadm.
Panel LCD del chasis	Use la pantalla LCD en el panel frontal para realizar lo siguiente: • Visualizar alertas e IP del CMC. • Configure DHCP. • Configure los valores de dirección IP estática del CMC. • Ver la dirección MAC del CMC para el CMC activo. • Ver la Id. de VLAN del CMC agregada al final de la dirección IP del CMC si la VLAN ya está configurada.
Telnet	Proporciona acceso de la línea de comandos a la CMC a través de la red. La interfaz de línea de comandos RACADM y el comando `connect`, que se utiliza para conectar a la consola serie de un servidor o módulo de E/S, están disponibles desde la línea de comandos de la CMC. **NOTA: Telnet no es un protocolo seguro y está desactivado de manera predeterminada. Transmite todos los datos, incluidas las contraseñas, en texto sin formato. Al transmitir información confidencial, utilice la interfaz SSH.**

Interfaz	Descripción
SSH	Use SSH para ejecutar comandos RACADM. SSH proporciona las mismas capacidades que la consola Telnet, pero utiliza una capa de transporte cifrado para mayor seguridad. El servicio SSH está activado de forma predeterminada en el CMC y se puede desactivar.
WSMan	Los servicios WSMan se basan en el protocolo Web Services for Management (WSMan) para realizar tareas de administración de uno a varios sistemas. Debe utilizar el cliente WSMan como cliente WinRM (Windows) o el cliente OpenWSMan (Linux) para utilizar la funcionalidad de servicios CMC. También puede utilizar Power Shell y Python para crear secuencias de comandos para la interfaz WSMan. WSMan es un protocolo basado en el Protocolo simple de acceso a objetos (SOAP) que se utiliza para la administración de sistemas. La CMC utiliza WS–Management para transmitir información de administración basada en el modelo común de información (CIM) de Distributed Management Task Force (DMTF). La información CIM define la semántica y los tipos de información que se pueden modificar en un sistema administrado. La implementación WSMan de la CMC usa SSL en el puerto 443 para la seguridad de transporte y admite la autentificación básica. Los datos disponibles a través de WS-Management se proporcionan con la interfaz de instrumentación del CMC asignada a los perfiles de DMTF y los perfiles de extensión. Para obtener más información, ver: • MOF y perfiles: **delltechcenter.com/page/DCIM.Library** • Sitio web de DTMF: **dmtf.org/standards/profiles/** • Archivo de WSMan Release notes. • **www.wbemsolutions.com/ws_management.html** • Especificaciones DMTF para WSManagement: **www.dmtf.org/standards/wbem/wsman** Las interfaces de servicios web pueden utilizarse aprovechando la infraestructura cliente, como Windows WinRM y Powershell CLI, utilidades de código fuente abierto como WSManCLI y entornos de programación de aplicaciones como Microsoft .NET. La herramienta WinRM establece una respuesta predeterminada de expiración de tiempo de 60 segundos para todos los comandos de WSMan que envía. WinRM no permite variaciones en este intervalo de expiración de tiempo. Usar "winrm set winrm/config @{MaxTimeoutms ="80000"}" no cambia la expiración de tiempo debido a un error en la herramienta WinRM. Por lo tanto, se recomienda no usar WinRM para los comandos que puedan tardar más de un minuto en completar la ejecución. Se recomienda el uso de bibliotecas que creen paquetes de SOAP-XML, ya que los usuarios pueden configurar la duración de la expiración de tiempo mediante dichas bibliotecas. Para establecer una conexión de cliente mediante Microsoft WinRM, la versión mínima requerida es 2.0. Para obtener más información, consulte el artículo de Microsoft, <**support.microsoft.com/kb/968929**>.

NOTA: Los valores predeterminados del nombre de usuario y la contraseña de la CMC son `root` y `calvin` respectivamente.

Inicio del CMC mediante otras herramientas de Systems Management

También es posible iniciar la CMC desde Dell Server Administrator o Dell OpenManage Essentials.

Para obtener acceso a la interfaz de la CMC mediante Dell Server Administrator, inicie Server Administrator en la estación de administración. En el panel izquierdo de la página de inicio de Server Administrator, haga clic en **Sistema** > **Chasis del sistema principal** >

Remote Access Controller. Para obtener más información, consulte *Dell Server Administrator User´s Guide* (Guía de usuario de Dell Server Administrator) disponible en **dell.com/support/manuals**.

Descarga y actualización de firmware del CMC

Para descargar el firmware del CMC, consulte Downloading CMC Firmware (Descarga de firmware del CMC).

Para actualizar el firmware del CMC, consulte Updating CMC Firmware (Actualización de firmware del CMC).

Configuración de la ubicación física del chasis y el nombre del chasis

Puede establecer el nombre del chasis y su ubicación en un centro de datos para poder identificarlo en la red (el nombre predeterminado es **Sistema de bastidor Dell**). Por ejemplo, una consulta SNMP sobre el nombre del chasis devuelve el nombre que haya configurado.

Configuración de la ubicación física del chasis y el nombre del chasis mediante la interfaz web

Para configurar la ubicación física del chasis y el nombre del chasis mediante la interfaz web de la CMC:

1 En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Configuración**.

2 En la página **Configuración general del chasis**, ingrese las propiedades de la ubicación y el nombre del chasis. Para obtener más información sobre las descripciones de los campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

> **NOTA: El campo Ubicación del chasis es opcional. Se recomienda usar los campos Centro de datos, Pasillo, Bastidor y Ranura de bastidor para indicar la ubicación física del chasis.**

3 Haga clic en **Aplicar**. La configuración se guarda.

Configuración de la ubicación física del chasis y el nombre del chasis mediante RACADM

Para establecer el nombre del chasis, la ubicación y la fecha y hora mediante la interfaz de línea de comandos, consulte los comandos **setsysinfo** y **setchassisname**. Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Establecimiento de la fecha y la hora en el CMC

Es posible establecer la fecha y la hora manualmente, o sincronizar la fecha y la hora con un servidor de protocolo de hora de red (NTP).

Establecimiento de la fecha y la hora en el CMC mediante la interfaz web del CMC

Para establecer la fecha y hora en la CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Configuración** > **Fecha/Hora**.

2 Para sincronizar la fecha y la hora con un servidor de protocolo de hora de red (NTP), en la página **Fecha/hora**, seleccione **Activar NTP** y especifique hasta tres servidores NTP. Para establecer manualmente la fecha y la hora, deje en blanco la opción **Activar NTP** y, a continuación, edite los campos **Fecha** y **Hora**.

3 Seleccione la **zona horaria** en el menú desplegable y haga clic en **Aplicar**.

Establecimiento de la fecha y la hora en el CMC mediante RACADM

Para establecer la fecha y la hora con la interfaz de la línea de comandos, consulte las secciones de grupo de propiedades de base de datos `cfgRemoteHosts` y del comando **config** en *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Configuración de los LED para identificar componentes en el chasis

Es posible activar los LED de los componentes (chasis, servidores, unidades de discos físicos, discos virtuales y módulos de E/S) para que parpadeen a fin de poder identificar el componente en el chasis.

NOTA: Para modificar esta configuración, es necesario contar con privilegios de Administrador de configuración del chasis.

Configuración del parpadeo de LED mediante la interfaz web del CMC

Para activar el parpadeo de los LED de uno, varios o todos los componentes:

- En el panel izquierdo, vaya a una de las siguientes páginas:
  - **Descripción general del chasis** > **Solución de problemas**.
  - **Descripción general del chasis** > **Controladora del chasis** > **Solución de problemas**.
  - **Descripción general del chasis** > **Descripción general del servidor** > **Solución de problemas**.

    NOTA: Solamente se pueden seleccionar servidores en esta página.
  - **Descripción general del chasis** > **Descripción general del módulo de E/S** > **Solución de problemas**.
  - **Almacenamiento** > **Solución de problemas** > **Identificar**.

    NOTA: En esta página se puede seleccionar disco físico por gabinetes, discos virtuales por gabinetes y LED del componente de almacenamiento externo.

Para activar el parpadeo del LED de un componente, seleccione la opción **Seleccionar/Deseleccionar todo** correspondiente a la unidad de disco físico o disco virtual o gabinetes y, a continuación, haga clic en **Hacer parpadear**. Para desactivar el parpadeo del LED de un

componente, deje en blanco la opción **Seleccionar/Deseleccionar todo** correspondiente al LED y, a continuación, haga clic en **Dejar de parpadear**.

Configuración del parpadeo de LED a través de RACADM

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

`racadm setled -m <module> [-l <ledState>]`, donde `<module>` especifica el módulo cuyo LED desea configurar. Las opciones de configuración son:

- `server-n` donde *n* = 1-4
- `switch-1`
- `cmc-active`

y `<ledState>` especifica si el LED debe parpadear o no. Las opciones de configuración son:

- 0: Sin parpadear (valor predeterminado)
- 1: Parpadeando

`racadm raid <operation> <component FQDD>`, donde el valor *operation* es `blink` o `unblink` y el FQDD es para la unidad de disco físico, el disco virtual y los gabinetes del componente.

Configuración de las propiedades del CMC

Puede configurar las propiedades de la CMC, como el presupuesto de alimentación, la configuración de red, los usuarios y las alertas de SNMP y por correo electrónico utilizando la interfaz web o RACADM.

Configuración del método de inicio del iDRAC con la interfaz web del CMC

Para configurar el método de inicio del iDRAC desde la página **Configuración general del chasis**:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Configuración**.
   Aparecerá la página **Configuración general del chasis**.
2. En el menú desplegable de la propiedad **Método de inicio del iDRAC**, seleccione **Dirección IP** o **DNS**.
3. Haga clic en **Aplicar**.

NOTA: Se usará un inicio basado en DNS para cualquier iDRAC particular solo en los siguientes casos:

- La configuración del chasis es DNS.
- El CMC ha detectado que el iDRAC específico está configurado con un nombre de DNS.

Configuración del método de inicio de iDRAC con RACADM

Para actualizar el firmware de la CMC mediante RACADM, utilice el subcomando `cfgRacTuneIdracDNSLaunchEnable`. Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Configuración de los atributos de la política de bloqueo de inicio de sesión con la interfaz web del CMC

NOTA: Para realizar las siguientes tareas, debe tener privilegios de Administrador de configuración del chasis.

La **Seguridad de inicio de sesión** le permite configurar los atributos de rango de IP para inicio de sesión de la CMC mediante la interfaz web de la CMC. Para configurar los atributos de rango de IP mediante la interfaz web del CMC:

1. En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Red** > **Red**.
   Aparecerá la página **Configuración de red**.
2. En la sección Configuración de IPv4, haga clic en **Opciones avanzadas**. De manera alternativa, para acceder a la página **Seguridad de inicio de sesión**, en el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en**Seguridad** > **Inicio de sesión**.
   Aparecerá la página **Seguridad de inicio de sesión**.
3. Para activar la función de bloqueo de usuarios o bloqueo de IP, en la sección **Política de bloqueo de inicio de sesión**, seleccione **Bloqueo por nombre de usuario** o **Bloqueo por dirección IP (IPV4)**.
   Se activarán las opciones para configurar los otros atributos de la política de bloqueo de inicio de sesión.
4. Introduzca los valores requeridos de los atributos de la política de bloqueo de inicio de sesión en los campos activados: **Bloqueo por conteo de intentos fallidos**, **Ventana de bloqueo por intentos fallidos** y **Bloqueo por tiempo de penalidad**. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para la CMC)*.
5. Para guardar estas opciones, haga clic en **Aplicar**.

Configuración de los atributos de la política de bloqueo de inicio de sesión con RACADM

Puede usar RACADM configurar las siguientes funciones de los atributos de la política de bloqueo de inicio de sesión:

- Bloqueo de usuarios
- Bloqueo de direcciones IP
- Cantidad de intentos de inicio de sesión permitidos
- Periodo de tiempo dentro del cual se producirán los conteos de bloqueo por inicio de sesión fallido
- Bloqueo por tiempo de penalidad

- Para activar la función de bloqueo de usuarios, use:
  ```
  racadm config -g cfgRacTuning -o  cfgRacTuneUserBlkEnable <0|1>
  ```
- Para activar la función de bloqueo de direcciones IP, use:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIPBlkEnable <0|1>
  ```
- Para especificar la cantidad de intentos de inicio de sesión, use:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount
  ```
- Para especificar el periodo de tiempo dentro del cual deben producirse los conteos de bloqueo por inicio de sesión fallido, use:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow
  ```
- Para especificar el valor del bloqueo por tiempo de penalidad, use:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime
  ```

Para obtener más información acerca de estos objetos, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Descripción del entorno de CMC redundante

Puede instalar una CMC en espera que asuma el control si la CMC activa deja de funcionar. La CMC redundante puede estar instalada previamente o se puede instalar posteriormente. Para garantizar la redundancia completa o el mejor rendimiento, es importante que la red de la CMC esté conectada correctamente

Las protecciones contra fallas pueden ocurrir cuando:

- Ejecute el comando `cmcchangeover` de RACADM. Consulte la sección del comando `cmcchangeover` en la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en dell.com/support/manuals.
- Ejecute el comando `racreset` de RACADM en la CMC activa. Consulte la sección del comando `racreset` en la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en dell.com/support/manuals.
- Restablezca la CMC activa desde la interfaz web. Consulte la opción `Reset CMC` para **Operaciones de control de alimentación** que se describe en Ejecución de las operaciones de control de alimentación.
- Desconecta el cable de red del CMC activo.
- Desmonta el CMC activo del chasis.
- Inicia una actualización del firmware del CMC en el CMC activo.
- Cuenta con un CMC activo que ya no está en estado funcional.

NOTA: En caso de conmutación por error en la CMC, se cerrarán todas las conexiones del iDRAC y todas las sesiones activas de la CMC. Los usuarios con sesiones cerradas deberán volver a conectarse a la nueva CMC activa.

Acerca del CMC en espera

La CMC en espera es idéntica a la CMC activa, y se mantiene como un reflejo de esta última. Las CMC activa y en espera deben tener instalada la misma revisión de firmware. Si las revisiones de firmware son diferentes, el sistema informará que existe una "redundancia degradada".

La CMC en espera asume las mismas propiedades y configuración de la CMC activa. Se debe mantener la misma versión de firmware en ambas CMC, pero no es necesario duplicar los valores de configuración en la CMC en espera.

NOTA: Para obtener información sobre cómo instalar una CMC, consulte *el Manual de propietario de VRTX*. Para obtener instrucciones para la instalación del firmware de la CMC en espera, consulte Actualización del firmware.

Modo a prueba de fallos de CMC

El gabinete PowerEdge VRTX habilita el modo a prueba de errores para proteger los servidores y el módulo de E/S de errores. El modo a prueba de errores se habilita cuando no hay ninguna CMC controlando el chasis. Durante el período de conmutación por error de la CMC o durante la pérdida de administración de una sola CMC:

- No se pueden encender los servidores recientemente instalados.
- No se puede acceder de forma remota a los servidores existentes.
- El rendimiento del servidor se reduce para limitar el consumo de energía hasta que se restaure la administración del CMC.

A continuación se indican algunas de las condiciones que pueden provocar la pérdida de administración de un CMC:

- Extracción del CMC: la administración del chasis se reanuda después de que se reemplaza el CMC o se ejecuta una protección contra fallas al CMC en espera.
- Extracción del cable de red de la CMC o pérdida de la conexión de red: la administración del chasis se reanuda después de que el chasis realiza una conmutación por error a la CMC en espera. La conmutación por error a la red solo se activa en modo de CMC redundante.

- Restablecimiento del CMC: la administración del chasis se reanuda después de que se reinicia el CMC o el chasis cede el control al CMC en espera después de una falla.
- Emisión del comando de protección contra fallas del CMC: la administración del chasis se reanuda después de que el chasis cede el control al CMC en espera después de una falla.
- Actualización del firmware de la CMC: la administración del chasis se reanuda después de que se reinicia la CMC o el chasis cede el control al CMC en espera después de una falla. Se recomienda actualizar primero la CMC en espera, de manera que solo haya un evento de conmutación por error.
- Detección y corrección de errores del CMC: la administración del chasis se reanuda después de que se reinicia el CMC o el chasis cede el control al CMC en espera después de una falla.

NOTA: El gabinete se puede configurar con un CMC sencillo o con CMC redundantes. En las configuraciones de CMC redundante, si la CMC principal pierde la comunicación con el gabinete o la red de administración, el CMC en espera asume la administración del chasis.

Proceso de elección del CMC activo

No hay ninguna diferencia entre las dos ranuras de la CMC; es decir, la ranura no indica prioridad. En lugar de eso, la CMC que se instala o se inicia primero asume la función de una CMC activa. Si se aplica alimentación de CA con dos CMC instaladas, la CMC instalada en la ranura 1 del chasis de la CMC generalmente asume la función activa. La CMC activa está indicada con un LED azul.

Si se insertan dos CMC en un chasis que ya está encendido, la negociación automática de activo/en espera puede requerir hasta dos minutos. El funcionamiento normal del chasis se reanuda cuando se completa la negociación.

Obtención del estado de condición del CMC redundante

Es posible ver el estado de la CMC en espera en la interfaz web. Para obtener más información sobre el acceso al estado de la CMC en la interfaz web, consulte Visualización de información del chasis y supervisión de la condición de los componentes y del chasis.

Configuración del panel frontal

Puede configurar los siguientes atributos:

- Botón de encendido
- LCD
- Unidad de DVD

Configuración del botón de encendido

Para configurar el botón de encendido del chasis:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Panel frontal** > **Configuración**.

2 En la página **Configuración del panel frontal**, en la sección **Configuración del botón de encendido**, seleccione la opción **Desactivar botón de encendido del chasis** y, a continuación, haga clic en **Aplicar**.

El botón de encendido del chasis está desactivado.

Configuración del LCD

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Panel frontal** > **Configuración**.

2 En la página **Configuración**, vaya a la sección **Configuración de LCD** y realice lo siguiente:

- Seleccione la opción **Bloquear LCD de panel de control** para desactivar cualquier configuración que se pueda realizar con la interfaz del LCD.
- Seleccione el idioma en el menú desplegable **Idioma de LCD**.
- En el menú desplegable **Orientación de LCD**, seleccione el modo requerido: **modo de torre** o **modo de bastidor**.

NOTA: Cuando configura el chasis mediante el asistente del LCD, si selecciona la opción Aplicar automáticamente la configuración a los servidores recientemente insertados, no puede desactivar la función Aplicar automáticamente la configuración a los servidores recientemente insertados con una licencia básica. Si no desea que la función se vuelva efectiva, ignore el mensaje que aparece en el LCD, el cual desaparecerá en forma automática; o bien, presione el botón No aceptar en el LCD y, a continuación, presione el botón central.

3 Haga clic en **Aplicar**.

Acceso a un servidor mediante KVM

Para asignar el servidor al KVM y activar el acceso a la consola remota del servidor a través de la interfaz de KVM, se puede utilizar la interfaz web del CMC, RACADM o la interfaz del LCD.

Asignación de un servidor a KVM mediante la interfaz web del CMC

Asegúrese de que la consola KVM esté conectada al chasis.
Para asignar un servidor a un KVM:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Panel frontal** > **Configuración**.
2 En la página **Configuración del panel anterior**, dentro de la sección **Configuración de KVM**, en la lista **KVM asignado**, seleccione la ranura que se debe asignar a un KVM y, a continuación, haga clic en **Aplicar**.

NOTA: El KVM permite la asignación a todas las ranuras de servidor. Si inserta un servidor de altura completa o reemplaza un servidor de mitad de altura por otro de altura completa, ello no afecta el comportamiento de la asignación. Sin embargo, si el KVM está asignado a una ranura inferior y la ranura tiene un servidor de altura completa, el KVM solo está disponible a través de la ranura superior. Debe reasignar el KVM a las ranuras superiores.

Asignación del servidor a KVM mediante la interfaz del LCD

Asegúrese de que la consola KVM esté conectada al chasis.
Para asignar el servidor a KVM mediante la interfaz del LCD: en la pantalla **Menú principal** en el LCD, vaya a **Asignación de KVM**, seleccione el servidor que se debe asignar y, a continuación, presione Aceptar.

Asignación de un servidor a una unidad de DVD

Para asignar el servidor a la unidad de DVD del chasis:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Panel frontal** > **Configuración**.
2 En la página **Configuración del panel anterior**, dentro de la sección **Configuración de la unidad de DVD**:
En el menú desplegable **DVD asignado**, seleccione uno de los servidores: Seleccione los servidores para los cuales se requiere acceso a la unidad de DVD del chasis.
3 Haga clic en **Aplicar**.

El DVD permite la asignación a todas las ranuras de servidor. Si inserta un servidor de altura completa o se reemplaza un servidor de mitad de altura por otro de altura completa, ello no afecta el comportamiento de la asignación. Sin embargo, si el DVD está asignado a una ranura inferior y la ranura tiene un servidor de altura completa, el DVD solo está disponible a través de la ranura superior. Debe reasignar el DVD a las ranuras superiores.

3

Inicio de sesión en el CMC

Puede iniciar sesión en la CMC como un usuario local de la CMC, como usuario del Active Directory de Microsoft o como usuario del LDAP. El nombre de usuario y la contraseña predeterminados son `root` y `calvin` respectivamente. También puede iniciar sesión mediante el inicio de sesión único o la tarjeta inteligente.

NOTA: La controladora CMC no admite los siguientes caracteres especiales como nombre de usuario o contraseña del perfil del chasis mediante XML:

" , ! , #, $, %, ^, &, *, (,), -, _, +, =, ?, {, }, +, &, >, |, .., ', [

Temas:

Acceso a la interfaz web del CMC

Antes de iniciar sesión en el CMC mediante la interfaz web, asegúrese de haber configurado un explorador web compatible (Internet Explorer o Firefox) y que la cuenta de usuario se haya creado con los privilegios necesarios.

NOTA: Si usa Microsoft Internet Explorer, con conexión a través de un proxy y recibe el error `The XML page cannot be displayed`, deberá desactivar el proxy para continuar.

Para acceder a la interfaz web de la CMC:

1. Abra un explorador web compatible en el sistema.

   Para obtener información actualizada sobre los exploradores web admitidos, consulte *Dell Systems Software Support Matrix (Matriz de compatibilidad de software de los sistemas Dell)* que se encuentra en **dell.com/support/manuals**.
2. En el campo **Dirección**, escriba la siguiente dirección URL y presione <Intro>:
   - Para acceder a la CMC a través de la dirección IPv4: `https://<CMC IP address>`

     Si el número de puerto HTTPS predeterminado (puerto 443) se modificó, escriba: `https://<CMC IP address>:<port number>`
   - Para acceder a la CMC a través de la dirección IPv6: `https://[<CMC IP address>]`

     Si se cambió el número de puerto HTTPS predeterminado (puerto 443), escriba: `https://[<CMC IP address>]:<port number>`, donde *<CMC IP address>* es la dirección IP para CMC y *<port number>* es el número de puerto HTTPS.

Aparecerá la página **Inicio de sesión de CMC**.

NOTA: Cuando utilice IPv6, deberá poner el valor de la dirección IP de CMC entre corchetes ([ ]).

Inicio de sesión en el CMC como usuario local, usuario de Active Directory o usuario de LDAP

Para iniciar sesión en la CMC, debe tener una cuenta de la CMC con el privilegio **Iniciar sesión en la CMC**. El nombre de usuario predeterminado del CMC es root y la contraseña, calvin. La cuenta raíz es la cuenta de administración predeterminada que se envía con el CMC.

NOTA:

- Para mayor seguridad, se recomienda cambiar la contraseña predeterminada de la cuenta raíz durante la configuración inicial.
- Cuando la validación de certificados está activada, debe proporcionar el FQDN del sistema. Si está activada la validación de certificados y se proporciona la dirección IP para la controladora de dominio, el inicio de sesión falla.

El CMC no admite caracteres ASCII extendidos, como ß, å, é, ü u otros caracteres utilizados principalmente en idiomas distintos al inglés.

Para iniciar sesión como usuario local, usuario de Active Directory o usuario LDAP:

1 En el campo **Nombre de usuario**, escriba su nombre de usuario:
   - Nombre de usuario de CMC: <nombre de usuario>
   - Nombre de usuario de Active Directory: <dominio>\<nombre de usuario>, <dominio>/<nombre de usuario> o bien <usuario>@<dominio>.
   - Nombre de usuario de LDAP: <nombre de usuario>

   NOTA: Este campo distingue entre mayúsculas y minúsculas.
2 En el campo **Contraseña**, escriba la contraseña de usuario.

   NOTA: Para usuario de Active Directory, el campo Nombre de usuario distingue entre mayúsculas y minúsculas.
3 En el menú desplegable del campo **Dominio**, seleccione el dominio requerido.
4 De forma opcional, seleccione un límite de tiempo de espera para la sesión. Este es el período durante el cual puede permanecer conectado sin actividad antes de que el sistema cierre la sesión automáticamente. El valor predeterminado es el **Tiempo de espera sin actividad del servicio web.**
5 Haga clic en **OK** (Aceptar).

   Iniciará sesión en la CMC con los privilegios de usuario necesarios.

   No puede iniciar sesión en la interfaz web con diferentes nombres de usuarios en varias ventanas del explorador en una sola estación de trabajo.

NOTA: Si está habilitada la autentificación LDAP e intenta iniciar sesión en la CMC mediante las credenciales locales, estas se comprueban en primer lugar en el servidor LDAP y, a continuación, en la CMC.

Inicio de sesión en el CMC mediante una tarjeta inteligente

Para usar esta función, debe tener una licencia Enterprise. Puede iniciar sesión en la CMC mediante una tarjeta inteligente. Las tarjetas inteligentes proporcionan Autenticación de dos factores (TFA) que ofrecen dos capas de seguridad.

- Dispositivo de tarjeta inteligente física.
- Código secreto, tal como una contraseña o un PIN.

Los usuarios deben verificar sus credenciales mediante la tarjeta inteligente y el PIN.

NOTA: No se puede utilizar la dirección IP para iniciar sesión en la CMC con el inicio de sesión mediante tarjeta inteligente. Kerberos valida sus credenciales en función del Nombre de dominio plenamente calificado (FQDN).

Antes de iniciar sesión como usuario de Active Directory mediante una tarjeta inteligente, asegúrese de realizar lo siguiente:

- Cargar un certificado de CA de confianza (certificado de Active Directory firmado por una autoridad de certificados) en la CMC.
- Configurar el servidor DNS.
- Activar el inicio de sesión de Active Directory.
- Activar el inicio de sesión mediante tarjeta inteligente.

Para iniciar sesión en la CMC como usuario de Active Directory mediante una tarjeta inteligente:

1 Inicie sesión en la CMC mediante el enlace `https://<cmcname.domain-name>`

Aparecerá la página **Inicio de sesión de CMC** en la que se le solicitará que inserte la tarjeta inteligente.

NOTA: Si ha cambiado el número del puerto HTTPS predeterminado (puerto 80), visite la página web de la CMC mediante `<cmcname.domain-name>:<port number>`, donde cmcname es el nombre de host de la CMC, *domain-name* es el nombre del dominio y *port number* es el número del puerto HTTPS.

2 Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.

Se muestra el cuadro de diálogo PIN.

3 Introduzca el PIN y haga clic en **Enviar**.

NOTA: Si el usuario de la tarjeta inteligente está presente en Active Directory, no es necesario introducir una contraseña de Active Directory. De lo contrario, debe iniciar sesión mediante un nombre de usuario y una contraseña adecuados.

Habrá iniciado sesión en la CMC mediante las credenciales de Active Directory.

Inicio de sesión en el CMC mediante el inicio de sesión único

Cuando se activa el inicio de sesión único (SSO), es posible iniciar sesión en la CMC sin introducir las credenciales de autenticación de usuario del dominio, como el nombre de usuario y la contraseña. Para usar esta función, debe tener una licencia Enterprise.

NOTA: No se puede utilizar la dirección IP para realizar el inicio de sesión único. Kerberos valida sus credenciales en función del Nombre de dominio plenamente calificado (FQDN).

Antes de iniciar sesión en la CMC mediante inicio de sesión único, asegúrese de que:

- Ha iniciado sesión en el sistema mediante una cuenta de usuario de Active Directory válida.
- La opción de inicio de sesión único está activada durante la configuración de Active Directory.

Para iniciar sesión en la CMC mediante inicio de sesión único:

1 Inicie sesión en el sistema cliente utilizando la cuenta de red.

2 Acceda a la interfaz web de la CMC por medio de: `https://<cmcname.domain-name>`

Por ejemplo, **cmc-6G2WXF1.cmcad.lab,** donde **cmc-6G2WXF1** es el nombre de cmc y **cmcad.lab** es el nombre de dominio.

NOTA: Si ha cambiado el número del puerto HTTPS predeterminado (puerto 80), obtenga acceso a la interfaz web de la CMC mediante `<cmcname.domain-name>:<port number>`, donde *cmcname* es el nombre de host de la CMC, domain-name es el nombre del dominio y port number es el número del puerto HTTPS.

La CMC lo conectará utilizando las credenciales Kerberos que el explorador almacenó en caché cuando inició sesión utilizando su cuenta de Active Directory válida. Si la conexión no es exitosa, el explorador es redirigido a la página de inicio de sesión normal de la CMC.

NOTA: Si no inicia sesión en el dominio de Active Directory y utiliza un explorador diferente de Internet Explorar, el inicio de sesión no es exitoso y el explorador muestra una página solo en blanco.

Antes de iniciar sesión en el CMC mediante una consola serie, Telnet o SSH

Es posible iniciar sesión en el CMC a través de una conexión serie, Telnet o SSH.

Una vez que haya configurado el software de emulador de terminal de la estación de administración y el BIOS del nodo administrado, realice las tareas siguientes para iniciar sesión en el CMC:

1 Conéctese a la CMC con el software de emulación de terminal de la estación de administración.
2 Escriba el nombre de usuario y la contraseña para la CMC y, a continuación, presione <Intro>.
Ahora está conectado a la CMC.

Vínculos relacionados

Uso de una consola Telnet con la CMC
Configuración de Minicom de Linux
Uso de SSH con la CMC

Acceso al CMC mediante RACADM

RACADM proporciona un conjunto de comandos que permiten configurar y administrar la CMC mediante una interfaz de texto. Es posible obtener acceso a RACADM por medio de una conexión Telnet/SSH o de serie, a través de la consola Dell CMC en el KVM o de manera remota mediante la interfaz de línea de comandos RACADM instalada en una estación de administración.

La interfaz RACADM se clasifica de la siguiente manera:

- RACADM remoto: permite ejecutar comandos RACADM en una estación de administración con la opción -r y el nombre DNS o la dirección IP del CMC.

  NOTA: RACADM remoto se incluye en el *DVD Dell Systems Management Tools and Documentation* y se instala en una estación de administración.
- RACADM de firmware: permite iniciar sesión en la CMC por medio de una conexión de serie, Telnet o SSH. Con RACADM de firmware, se puede ejecutar RACADM que forma parte del firmware de la CMC.

Es posible utilizar comandos de RACADM remotos en secuencias de comandos para configurar varias CMC. No es posible ejecutar las secuencias directamente en el interfaz web de la CMC, porque la CMC no la admite.

Para obtener más información acerca de RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX).

Para obtener más información sobre la configuración e varios CMC, consulte Configuring Multiple CMCs Using RACADM (Configuración de varios CMC mediante RACADM).

Inicio de sesión en el CMC mediante la autentificación de clave pública

Es posible iniciar sesión en la CMC a través de SSH sin introducir ninguna contraseña. También puede enviar un único comando RACADM como argumento de línea de comandos a la aplicación SSH. Las opciones de línea de comandos presentan un comportamiento similar a las de RACADM remoto, ya que la sesión termina una vez completado el comando.

Antes de iniciar sesión en el CMC a través de SSH, asegúrese de que las claves públicas estén cargadas. Para usar esta función, debe tener una licencia Enterprise.

Por ejemplo:

- **Inicio de sesión**: `ssh service@<domain>` o, `ssh service@<IP_address>` donde IP_address es la dirección IP de la CMC.
- **Envío de comandos RACADM**: `ssh service@<domain> racadm getversion` y `ssh service@<domain> racadm getsel`

Al iniciar sesión con la cuenta de servicio, si se configuró una frase de contraseña durante la creación del par de claves pública o privada, es posible que se le indique que debe volver a introducir la frase de contraseña. Si la frase de contraseña se utiliza con las claves, los sistemas cliente que ejecutan Windows y Linux proporcionan métodos para automatizar el método. En los sistemas cliente que ejecutan Windows, se puede usar la aplicación Pageant. Esta aplicación se ejecuta en segundo plano y hace que la introducción de la frase de contraseña sea transparente. Para los sistemas cliente que ejecutan Linux, se puede usar el agente ssh. Para configurar y utilizar cualquiera de estas aplicaciones, consulte la documentación del producto correspondiente.

Varias sesiones en el CMC

Aquí se proporciona una lista de varias sesiones en la CMC posibles mediante el uso de las diversas interfaces.

Tabla 11. Varias sesiones en la CMC

Interfaz	Número de sesiones
Interfaz web del CMC	4
RACADM	4
Telnet	4
SSH	4

Cambio de la contraseña de inicio de sesión predeterminada

El mensaje de advertencia que le solicita cambiar la contraseña predeterminada se muestra si:

- Inicia sesión en el CMC con el privilegio **Configurar usuarios**.
- Está activada la función de advertencia de contraseña predeterminada.
- El nombre de usuario y la contraseña predeterminados para cualquiera de las cuentas activadas actualmente son `root` y `calvin`, respectivamente.

Se muestra el mismo mensaje de advertencia si inicia sesión con Active Directory o LDAP. Las cuentas de Active Directory y LDAP no se tienen en cuenta al momento de determinar si alguna cuenta (local) tiene `root` y `calvin` como credenciales. También aparece un mensaje de advertencia al iniciar sesión en la CMC con SSH, Telnet, RACADM remoto o la interfaz web. Para la interfaz web, SSH y Telnet, se muestra un solo mensaje de advertencia para cada sesión. Para RACADM remoto, se muestra el mensaje de advertencia para cada comando.

Para cambiar las credenciales, debe contar con el privilegio **Configurar usuarios**.

NOTA: Se genera un mensaje de inicio de sesión en el CMC si la opción No volver a mostrar esta advertencia está seleccionada en la página Inicio de sesión del CMC.

Cambio de la contraseña de inicio de sesión predeterminada mediante la interfaz web

Cuando se conecta a la interfaz web de la CMC, si aparece la página **Advertencia de contraseña predeterminada**, puede cambiar la contraseña. Para hacerlo:

1 Seleccione la opción **Cambiar contraseña predeterminada**.

2 En el campo **Contraseña nueva**, escriba la contraseña nueva.

La cantidad máxima de caracteres para la contraseña es 20. Los caracteres están enmascarados. Se admiten los siguientes caracteres:

- 0-9
- A-Z
- a-z
- Caracteres especiales: +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, l, \

3 En el campo **Confirmar contraseña**, escriba nuevamente la contraseña.

4 Haga clic en **Continue (Continuar)**. Se configura la contraseña nueva y queda conectado a la CMC.

NOTA: Continuar se activa solo si coinciden las contraseñas proporcionadas en los campos Contraseña nueva y Confirmar contraseña.

Para obtener información acerca del resto de los campos, consulte la *Ayuda en línea*.

Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM

Para cambiar la contraseña, ejecute el siguiente comando RACADM:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index> <newpassword>
```

donde, `<index>` es un valor de 1 a 16 (indica la cuenta de usuario) y `<newpassword>` es la contraseña nueva definida por el usuario.

Para obtener más información, consulte la *Guía de referencia sobre la línea de comando RACADM de Chassis Management Controller para PowerEdge VRTX* que está disponible en **dell.com/support/manuals**.

Activación o desactivación del mensaje de advertencia de contraseña predeterminada

Puede activar o desactivar la pantalla del mensaje de aviso de contraseña predeterminada. Para ello, debe contar con el privilegio **Configurar usuarios**.

Activación o desactivación del mensaje de advertencia de contraseña predeterminada mediante la interfaz web

Para activar o desactivar la visualización del mensaje de advertencia de contraseña predeterminada después de iniciar sesión en iDRAC:

1 Diríjase a **Controladora del chasis** > **Autentificación de usuarios** > **Usuarios locales**.

Se muestra la página **Users (Usuarios)**.

2 En la sección **Advertencia de contraseña predeterminada**, seleccione **Activar** y, a continuación, haga clic en **Aplicar** para activar la visualización de la página **Advertencia de contraseña predeterminada** cuando inicie sesión en el CMC. De lo contrario, seleccione **Desactivar**.

De manera alternativa, si esta función está activada y no desea que se muestre el mensaje de advertencia para las operaciones de inicio de sesión subsiguientes, vaya a la página **Advertencia de contraseña predeterminada**, seleccione la opción **No volver a mostrar esta advertencia** y haga clic en **Aplicar**.

Activación o desactivación del mensaje de advertencia para cambiar la contraseña de inicio de sesión predeterminada mediante RACADM

Para activar la visualización del mensaje de advertencia para cambiar la contraseña de inicio de sesión predeterminada mediante RACADM, utilice el objeto `racadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> or <1>`. Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Situaciones de uso

Esta sección describe los casos de uso y las tareas típicas que se pueden realizar con Chassis Management Controller versión 3.0 para Dell PowerEdge VRTX.

Conversión de tarjeta PERC 8 compartida externa de modo de alta disponibilidad a modo sin alta disponibilidad mediante la interfaz web

El chasis Dell PowerEdge VRTX debe tener 2 tarjetas PERC 8 compartidas externas en la ranura PCI 5 y la ranura PCI 6 en modo HA.

Flujo de trabajo

1. Encienda el chasis. Apague el chasis. Desconecte todos los cables SAS de las tarjetas PERC 8 compartidas externas a los gabinetes MD12x0.
2. Encienda el chasis.
3. Inicie sesión en la interfaz web de la CMC y desplácese a **Almacenamiento→ Controladoras→ Solución de problemas**y desactive **Tolerancia a errores** en el menú desplegable para tarjeta PERC 8 compartida externa en la ranura 5, haga clic en **Aplicar** y seleccione Desactivar para ranura 6 y, a continuación, haga clic en **Aplicar**.
4. El restablecimiento de ambas PERC puede tardar dos minutos en reflejarse en el modo sin alta disponibilidad.
5. Apague el chasis y conecte los gabinetes en modo sin alta disponibilidad.
6. Encienda el chasis.
7. La tarjeta PERC 8 compartida externa no está en modo de alta disponibilidad y vaya a **Almacenamiento→ Solución de problemas→ Configurar solución de problemas** para ver el estado sin alta disponibilidad.

Conversión de tarjeta PERC 8 compartida externa de modo de alta disponibilidad a modo sin alta disponibilidad mediante la interfaz web

El chasis Dell PowerEdge VRTX debe tener 2 tarjetas PERC 8 compartidas externas en la ranura PCI 5 y la ranura PCI 6.

Flujo de trabajo

1. Apague el chasis. Desconecte todos los cables SAS de las tarjetas PERC 8 compartidas externas a los gabinetes MD12x0.
2. Encienda el chasis.
3. Inicie sesión en la interfaz web de la CMC y desplácese a **Almacenamiento→ Controladoras→ Solución de problemas**y active **Tolerancia a errores** en el menú desplegable para la tarjeta PERC 8 compartida externa en la ranura 5, haga clic en **Aplicar** y seleccione Desactivar para la ranura 6 y, a continuación, haga clic en **Aplicar**.
4. El restablecimiento de ambas PERC puede tardar dos minutos para reflejarse en el modo HA (alta disponibilidad).
5. Apague chasis y conecte los gabinetes en modo HA.
6. Encienda el chasis.
7. La tarjeta PERC 8 compartida externa está en modo de alta disponibilidad y vaya a **Almacenamiento→ Solución de problemas→ Configurar solución de problemas** para ver el estado de HA.

Conversión de tarjeta PERC 8 compartida externa de modo de alta disponibilidad a modo sin disponibilidad mediante RACADM

El chasis Dell PowerEdge VRTX debe tener 2 tarjetas PERC 8 compartidas externas en la ranura PCI 5 y la ranura PCI 6 en modo HA.

Flujo de trabajo

1. Apague el chasis. Desconecte todos los cables SAS de las tarjetas PERC 8 compartidas externas a los gabinetes MD12x0.
2. Encienda el chasis.
3. Inicie sesión en el RACADM de la CMC y ejecute el siguiente comando cuando los servidores estén apagados:

   ```
   racadm  raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode None
   ```
4. Ejecute el comando en `racadm raid set controllers:RAID.ChassisSlot.6-1 -p HighAvailabilityMode None` la tarjeta PERC 8 compartida externa en la ranura 6.
5. El restablecimiento de ambas PERC puede tardar dos minutos para reflejarse en el modo HA (alta disponibilidad).
6. Apague el chasis y conecte los gabinetes en modo sin alta disponibilidad.
7. Encienda el chasis.
8. La tarjeta PERC 8 compartida externa no está en modo de alta disponibilidad y el siguiente comando se utiliza para ver el estado:

   ```
   racadm raid get controllers -o -p HighAvailabilityMode
   ```

Conversión de tarjeta PERC 8 compartida externa del modo sin alta disponibilidad al modo de alta disponibilidad mediante RACADM

El chasis Dell PowerEdge VRTX debe tener las tarjetas PERC 8 compartidas externas en la ranura PCI 5 y la ranura PCI 6.

Flujo de trabajo

1. Encienda el chasis. Apague el chasis. Desconecte todos los cables SAS de las tarjetas PERC 8 compartidas externas a los gabinetes MD12x0.
2. Encienda el chasis.
3. Inicie sesión en el RACADM de la CMC y ejecute el siguiente comando cuando los servidores estén apagados:

   ```
   racadm raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode ha
   ```
4. Ejecute el comando en `racadm raid set controllers:RAID.ChassisSlot.6-1 -p HighAvailabilityMode ha` tarjeta PERC 8 compartido externo en la ranura 6.

5 El restablecimiento de ambas PERC puede tardar dos minutos para reflejarse en el modo HA (alta disponibilidad).

6 Apague chasis y conecte los gabinetes en modo HA.

7 Encienda el chasis.

8 La tarjeta PERC 8 compartida externa se encuentra en modo de alta disponibilidad y el estados de HA se ve mediante el siguiente comando:

```
racadm raid get controllers -o -p HighAvailabilityMode
```

.

4

Actualización de firmware

Es posible actualizar el firmware para:

- CMC
- Infraestructura del chasis
- Firmware de dispositivo expansor VRTX o dispositivo expansor del plano posterior del almacenamiento de los gabinetes externos o integrados
- Discos físicos por gabinete

NOTA: Puede actualizar el firmware de la unidad de disco duro solo si es necesario.

Puede actualizar el firmware de los siguientes componentes de E/S y del servidor:

- Módulo de E/S
- BIOS
- iDRAC
- Lifecycle Controller
- Diagnósticos de 32 bits
- Driver Pack del sistema operativo
- Controladoras de interfaz de red
- Controladoras RAID en el módulo del servidor

NOTA: La actualización puede tardar varios minutos en terminar.

Temas:

Descarga de firmware del CMC

Antes de iniciar la actualización de firmware, descargue la última versión del firmware de la página web **support.dell.com** y guárdela en el sistema local.

Si está actualizando el firmware del chasis VRTX, se recomienda que actualice las versiones de firmware de los componentes del chasis en el siguiente orden:

1 El firmware de los componentes de blade
2 Firmware de la CMC
3 Firmware de infraestructura del chasis
4 Firmware de la PERC8 compartida (integrada y externa)
5 Firmware de plano posterior de almacenamiento interno y expansores del gabinete externo
6 Firmware de la unidad de disco duro (gabinetes externos e integrados)

Para obtener más información sobre la secuencia de actualización para el chasis VRTX, consulte *CMC Firmware 3.0 Release Notes* (Notas de la versión 3.0 del firmware del CMC) disponibles en **dell.com/cmcmanuals**.

Visualización de versiones de firmware actualmente instaladas

Es posible ver las versiones de firmware actualmente instaladas mediante la interfaz web del CMC o RACADM.

Visualización de versiones de firmware actualmente instaladas mediante la interfaz web del CMC

En la interfaz web de la CMC, vaya a cualquiera de las siguientes páginas para ver las versiones de firmware actuales:

- **Descripción general del chasis** > **Actualizar**
- **Descripción general del chasis** > **Controladora del chasis** > **Actualizar**
- **Descripción general del chasis** > **Descripción general del servidor** > **Actualización de los componentes del servidor.**
- **Descripción general del chasis** > **Descripción general del módulo de E/S** > **Actualizar**
- **Descripción general del chasis** > **Almacenamiento** > **Actualización de los componentes de almacenamiento**

La página **Actualización del firmware** muestra la versión actual del firmware para cada componente de la lista y permite actualizar el firmware a la revisión más reciente.

Si el chasis contiene un servidor de una generación anterior cuyo iDRAC se encuentra en modo de recuperación, o si la CMC detecta que un iDRAC contiene firmware dañado, el iDRAC de la generación anterior también aparece en la página **Actualización del firmware**.

Visualización de versiones de firmware actualmente instaladas mediante RACADM

Para ver la información de IP para iDRAC y CMC, y el servicio de CMC o la etiqueta de propiedad mediante RACADM, ejecute el subcomando `racadm getsysinfo` . Para obtener más información sobre otros comandos RACADM, consulte la *Guía de referencia sobre líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX*.

Actualización de firmware del CMC

Puede actualizar el firmware de la CMC mediante la interfaz web o RACADM. De forma predeterminada, la actualización de firmware conserva la configuración actual de la CMC. Durante el proceso de actualización, es posible restablecer la configuración de la CMC a los valores predeterminados de fábrica.

NOTA: Para actualizar el firmware del CMC, es necesario contar con privilegios de Administrador de configuración del chasis.

Si se utiliza una sesión de interfaz de usuario web para actualizar el firmware de los componentes del sistema, se debe establecer un valor suficientemente elevado de **Tiempo de espera (0, 60–10800)** para adecuarse al tiempo de transferencia de archivos. En algunos casos, es posible que el tiempo de transferencia de archivos de firmware sea de hasta 30 minutos. Para configurar el valor de Tiempo de espera en inactividad, consulte Configuración de servicios.

Durante las actualizaciones de firmware del CMC, es normal que algunas o todas las unidades de ventilador del chasis giren a una velocidad del 100%.

Si existen CMC redundantes instaladas en el chasis, se recomienda actualizar las dos CMC a la misma versión de firmware al mismo tiempo con una sola operación. Si el firmware de las CMC es diferente y se produce una protección contra fallas, se pueden producir resultados inesperados.

NOTA:

- El firmware del CMC no se puede actualizar para cualquier versión anterior que no sea 2.0 para un chasis que está configurado con 1600 W PSU.
- La actualización o la reversión del firmware de la CMC se admite solamente en las versiones de firmware 1.2, 1.25, 1.3, 1.31, 1.35, 1.36, 2.0, 2.01, 2.04 y más recientes. Con cualquier otra versión, primeramente realice la actualización a cualquiera de estas versiones y luego realice la actualización a la versión requerida.

Una vez que se ha cargado el firmware correctamente, la CMC activa se restablece y deja de estar disponible temporalmente. Si existe una CMC en espera, las funciones de las CMC en espera y activa se intercambiarán. La CMC en espera se convierte en la CMC activa. Si se aplica una actualización solo a la CMC activa, después de que el restablecimiento concluya, la CMC activa no ejecutará la imagen actualizada, solo la CMC en espera ejecutará dicha imagen. En general, se recomienda especialmente mantener versiones de firmware idénticas para las CMC activa y en espera.

Cuando se haya actualizado la CMC en espera, intercambie las funciones de la CMC de modo que la CMC recientemente actualizada pase a ser la CMC activa y la CMC con el firmware anterior pase al modo en espera. Para más información acerca del intercambio de funciones, consulte la sección del comando `cmcchangeover` en la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM Chassis Management Controller para PowerEdge VRTX). La ejecución de este comando ayuda a verificar que la actualización se haya realizado satisfactoriamente y que el firmware nuevo esté funcionando adecuadamente, antes de actualizar el firmware en la segunda CMC. Cuando ambas CMC se hayan actualizado, puede usar el comando `cmcchangeover` para restaurar las CMC a sus funciones anteriores. La revisión 2.x del firmware de la CMC actualiza la CMC principal y la CMC redundante sin ejecutar el comando `cmcchangeover`.

Durante las etapas finales del proceso de actualización del firmware en la CMC, la sesión del explorador y la conexión con la CMC se perderán temporalmente debido a que la CMC no está conectada a la red. La CMC genera la condición general del chasis como crítica debido a la caída temporal de la red. Cuando se reinicia la CMC después de unos minutos, inicie sesión en la misma. A continuación, la CMC genera la condición general del chasis como en buen estado y el enlace de red de la CMC pasa a estar activo. Una vez se haya restablecido, aparecerá la nueva versión del firmware en la página **Actualización del firmware**.

Para evitar la desconexión de otros usuarios durante un restablecimiento, notifique a los usuarios autorizados que puedan iniciar sesión en la CMC y verifique las sesiones activas en la página **Sesiones**. Para abrir la página **Sesiones**, haga clic en **Descripción general del chasis** en el panel izquierdo, haga clic en **Red** y luego en **Sesiones**.

Al transferir archivos hacia y desde la CMC, el ícono de transferencia de archivos gira durante la transferencia. Si el ícono no tiene animación, asegúrese de que el explorador esté configurado para permitir animaciones. Para más información sobre cómo permitir animaciones en el explorador, consulte Permitir animaciones en Internet Explorer.

NOTA: Si ha configurado la longitud del nombre de la ranura en más de 15 caracteres en la versión actual de CMC, cambiar a una versión anterior de firmware de CMC limita la longitud del nombre de la ranura a 15 caracteres.

Imagen de firmware del CMC firmado

Para VRTX CMC 2.0 y versiones posteriores, el firmware incluye una firma. El firmware de la CMC verifica de firma para garantizar la autenticidad del firmware cargado. El proceso de actualización de firmware es exitoso solo si la CMC autentifica que la imagen de firmware es una imagen válida del proveedor de servicio y no ha sido alterada. El proceso de actualización del firmware se detiene si la CMC no puede verificar la firma de la imagen de firmware cargada. Se registra un suceso de advertencia y se muestra el mensaje de error correspondiente.

Se puede realizar la verificación de la firma en las versiones 1.2 y posteriores del firmware de VRTX. Para actualizar el firmware a versiones de VRTX anteriores que 1.2, primero actualice el firmware a una versión de la CMC de VRTX que sea posterior o igual a 1.2, pero anterior a 2.0. Después de realizar la actualización, se puede realizar la actualización del firmware a versiones de VRTX sin firma anteriores.

Actualización de la CMC y del firmware de la placa base

Las capacidades compartidas de la tarjeta PERC8 compartida externa no están disponibles hasta tanto no se actualice el firmware de la CMC y de la placa base.

NOTA:

- Para ver el diagrama de cableado MD12x0, consulte *Upgrading PowerEdge VRTX to Support Shared Storage Expansion User's Guide* (Guía del usuario de Actualización de PowerEdge VRTX para admitir expansión de almacenamiento compartido) o *Dell Shared PowerEdge RAID Controller (PERC) 8 Cards for Dell PowerEdge VRTX Systems User's Guide* (Guía del usuario de tarjetas Dell Shared PowerEdge RAID Controller (PERC) 8 para sistemas Dell PowerEdge VRTX) disponible en dell.com/support/manuals.
- El adaptador de almacenamiento compartido externo requiere que actualice la CMC v2.10 o posterior y placa base v2.21 o posterior para admitir la tarjeta PERC 8 compartida externa.
- No puede degradar el firmware de la CMC anterior a 2.2 con adaptadores compartidos externos.

Para actualizar el firmware de la CMC y la placa base:

1 Actualización de firmware del CMC.
2 Actualice el firmware de la placa base.
3 Apague el chasis e instale los adaptadores de almacenamiento compartido en la ranura PCIe 5 y 6.
4 Encienda el chasis.
5 Después de encender el chasis, actualice los adaptadores de almacenamiento compartido externo.

NOTA: De manera predeterminada, la tarjeta PERC 8 compartida externa está en modo de no tolerancia a errores. Se debe cambiar al modo de tolerancia de errores después de que se haya cableado adecuadamente. Para obtener más información, consulte *Actualización de PowerEdge VRTX para admitir la expansión de almacenamiento compartido*.

En un suceso, si desea revertir el firmware de la CMC o de MPC/placa base o la versión de firmware de la CMC y MPC, realice las siguientes tareas:

Para revertir el firmware de la CMC y de la placa base:

1 Apague el chasis.
2 Extraiga todos los adaptadores de almacenamiento externos de las ranuras PCI.
3 Encienda el chasis.

4 Revierta el firmware de la CMC o la placa base.

No puede degradar la CMC si se detecta el adaptador de almacenamiento compartido externo.

Si los procesos no se siguen en orden, el comportamiento del sistema se vuelve aleatorio y algunas piezas del sistema pueden volverse inestables. La CMC registra mensajes de la controladora IOV o RAID. Solo las asignaciones de VA de almacenamiento compartido para PERC 1 y PERC 2 son visibles en la versión anterior de la CMC. Todas las asignaciones de VA de almacenamiento compartido externo no existen en la versión anterior de la CMC. Si una tarjeta PERC 8 compartida externa se inserta después de la reversión, la CMC la considera como un adaptador no compartido. Puede ocurrir que el controlador PERC del HOST no admita la tarjeta PERC 8 compartida externa.

Actualización de firmware del CMC mediante la interfaz web

NOTA:

- Antes de aplicar la actualización del CMC, asegúrese de que el chasis esté encendido. Si los servidores blade están encendidos, no es necesario apagarlos para realizar la actualización de CMC.
- La degradación del firmware de la CMC anterior a 2.1 con adaptadores compartidos externos está bloqueada.

Para actualizar el firmware del CMC mediante la interfaz web del CMC:

1 En el panel izquierdo, vaya a una de las siguientes páginas:
   - **Descripción general del chasis** > **Actualizar**
   - **Descripción general del chasis** > **Controladora del chasis** > **Actualizar**
2 En la página **Actualización del firmware**, en la sección **Firmware del CMC**, seleccione los componentes requeridos en la columna **Actualizar destinos** para el CMC o los CMC (en caso de estar presente un CMC en estado de espera) que desea actualizar y haga clic en **Aplicar actualización del CMC**.
3 En el campo **Imagen del firmware**, haga clic en **Examinar** (Internet Explorer o Firefox) o **Seleccionar Archivo** (Google Chrome) para ir hasta la ubicación del archivo. El nombre predeterminado del archivo de la imagen del firmware de la CMC es `vrtx_cmc.bin`.
4 Haga clic en **Iniciar actualización del firmware**. La sección **Progreso de actualización del firmware** proporciona información sobre el estado de la actualización de firmware. Aparecerá un indicador de estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización de firmware.
5 En una CMC en espera, cuando finalice la actualización, el campo **Estado de la actualización** indicará **Listo**. En el caso de una CMC activa, durante las etapas finales del proceso de actualización del firmware, la sesión del explorador y la conexión con la CMC se perderán temporalmente debido a que la CMC activa no está conectada a la red. Debe iniciar sesión pasados unos minutos, cuando la CMC activa se haya reiniciado. Una vez que se haya restablecido, aparecerá el nuevo firmware en la página **Actualización del firmware**.

   NOTA: Después de la actualización del firmware, elimine los archivos de la memoria caché del explorador web. Para obtener instrucciones acerca de cómo borrar la memoria caché del explorador, consulte la ayuda en línea del explorador web.

Instrucciones adicionales:

- Durante una transferencia de archivos, no haga clic en el icono **Actualizar** ni navegue a otra página.
- Para cancelar el proceso, seleccione la opción **Cancelar transferencia y actualización de archivos**. Esta opción solo está disponible durante la transferencia de archivos.
- El campo **Estado de la actualización** muestra el estado de la actualización de firmware.

NOTA: Es posible que el proceso de actualización del CMC tarde varios minutos.

Actualización de firmware de la CMC mediante RACADM

Para actualizar el firmware de la CMC mediante RACADM, utilice el subcomando `fwupdate`. Para obtener más información sobre cómo usar comandos RACADM, consulte la *Guía de referencia sobre líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX*.

NOTA: Ejecute el comando de actualización del firmware a través de una sola sesión de racadm remota a la vez.

Actualización del firmware de infraestructura del chasis

La operación de actualización de infraestructura del chasis actualiza componentes, como el firmware de la placa principal y el firmware de administración del subsistema de PCIe.

NOTA: Para actualizar el firmware de infraestructura del chasis, asegúrese de que el chasis esté encendido y que los servidores estén apagados.

NOTA: Cuando la placa base se actualiza a una versión posterior, el chasis y Chassis Management Controller pueden reiniciarse.

Actualización del firmware de infraestructura del chasis mediante la interfaz web del CMC

1 Desplácese a cualquiera de las siguientes páginas:
   - **Descripción general del chasis** > **Actualizar**
   - **Descripción general del chasis** > **Controladora del chasis** > **Actualizar**
2 En la página **Actualización del firmware**, en la sección **Firmware de infraestructura del chasis**, en la columna **Actualizar destinos**, seleccione la opción y, a continuación, haga clic en **Aplicar firmware de infraestructura del chasis**.
3 En la página **Actualización del firmware**, haga clic en **Examinar** y seleccione el firmware de infraestructura del chasis correspondiente.
4 Haga clic en **Iniciar actualización del firmware** y, a continuación, en **Sí**.

   La sección **Progreso de actualización del firmware** proporciona información sobre el estado de la actualización de firmware. Mientras se carga el archivo de imagen, aparece un indicador de estado en la página. El tiempo para la transferencia de archivos puede variar según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización de firmware.

Instrucciones adicionales que hay que seguir:

- No haga clic en el icono **Actualizar** ni visite otra página durante la transferencia de archivos.
- El campo **Estado de la actualización** muestra el estado de la actualización de firmware.

Una vez finalizada la actualización, se produce una pérdida breve de conectividad en el dispositivo de módulo de E/S debido a su reinicio y se muestra el nuevo firmware en la página **Actualización del firmware**.

Actualización del firmware de la infraestructura del chasis mediante RACADM

Para actualizar el firmware de la infraestructura del chasis mediante RACADM, utilice el subcomando `fwupdate`. Para obtener más información sobre cómo usar comandos RACADM, consulte la *Guía de referencia sobre líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX*.

Actualización de firmware del iDRAC del servidor

Puede actualizar el firmware para iDRAC mediante la interfaz web de la CMC o RACADM. Para usar esta función, debe tener una licencia Enterprise.

La versión de firmware de iDRAC debe ser 1.40.40 o posterior para servidores con iDRAC.

iDRAC (en un servidor) se restablece y queda temporalmente no disponible después de una actualización del firmware.

NOTA: Para actualizar el firmware del iDRAC mediante Chassis Management Controller, debe haber una tarjeta SD disponible en el chasis. Sin embargo, para actualizar el firmware del iDRAC por medio de la interfaz web del iDRAC, no se necesita una tarjeta SD en la CMC. Para obtener más información sobre cómo iniciar la interfaz web del iDRAC desde la CMC, consulte Inicio del iDRAC desde la página de estado del servidor.

Actualización de firmware del iDRAC del servidor mediante la interfaz web

Para actualizar el firmware del iDRAC en el servidor:

1 Desplácese a cualquiera de las siguientes páginas:
- **Descripción general del chasis** > **Actualizar**.
- **Descripción general del servidor** > **Actualizar** > **Actualización de componentes del servidor**.

Se muestra la ventana **Actualización del firmware**.

NOTA:
También es posible actualizar el firmware del iDRAC a través de **Descripción general del chasis** > **Descripción general del servidor** > **Actualizar**. Para obtener más información, consulte Updating Server Component Firmware (Actualización del firmware de los componentes del servidor).

2 Para actualizar el firmware del iDRAC7 o del iDRAC8, en la sección **Firmware del iDRAC7** o **Firmware del iDRAC8** respectivamente, haga clic en el vínculo **Actualizar** correspondiente al servidor cuyo firmware desee actualizar.

Aparecerá la página **Actualización de los componentes del servidor**. Para continuar, consulte Actualización de firmware de los componentes del servidor.

3 En el campo **Imagen del firmware**, ingrese la ruta de acceso al archivo de la imagen del firmware en la estación de administración o la red compartida, o bien, haga clic en **Examinar** para navegar a la ubicación del archivo. El nombre de la imagen del firmware del iDRAC predeterminado es **firming.imc**.

4 Haga clic en **Iniciar actualización del firmware** y, a continuación, en **Sí**.

La sección **Progreso de actualización del firmware** proporciona información sobre el estado de la actualización de firmware. Una barra de progreso indica el estado del proceso de carga. El tiempo para la transferencia de archivos puede variar según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización de firmware.

NOTA: Instrucciones adicionales que hay que seguir:
- No haga clic en el icono **Actualizar** ni visite otra página durante la transferencia de archivos.
- Para cancelar el proceso, haga clic en **Cancelar transferencia y actualización de archivos**. Esta opción solo está disponible durante la transferencia de archivos.
- El campo **Estado de la actualización** muestra el estado de la actualización de firmware.

La actualización de firmware del iDRAC puede requerir de hasta 10 minutos.

Actualización de firmware de los componentes del servidor

La función de actualización de uno a varios en CMC permite actualizar el firmware de los componentes de varios servidores. Es posible actualizar los componentes del servidor mediante los paquetes de actualización Dell Update Packages disponibles en el sistema local o en un recurso compartido de red. Esta operación se activa mediante el aprovechamiento de la funcionalidad de Lifecycle Controller en el servidor.

El servicio Lifecycle Controller está disponible en cada servidor y es ofrecido por iDRAC. Puede administrar el firmware de los componentes y dispositivos en los servidores mediante el servicio Lifecycle Controller. Lifecycle Controller usa un algoritmo de optimización para actualizar el firmware que reduce la cantidad de reinicios de forma efectiva.

Lifecycle Controller admite la actualización de módulos para iDRAC7 y servidores posteriores.

NOTA: Antes de utilizar la función de actualización basada en Lifecycle Controller, se deben actualizar las versiones de firmware del servidor. También se debe actualizar el firmware de la CMC antes de actualizar los módulos de firmware de los componentes del servidor.

NOTA: Para actualizar el firmware de un componente, es necesario activar la opción CSIOR para servidores. Para activar CSIOR en:

- Servidores de 12ª generación y posteriores: después de reiniciar el servidor, en los valores de F2, seleccione **Configuración del iDRAC** > **Lifecycle Controller**, active **CSIOR** y guarde los cambios.
- Servidores de 13.ª generación: después de reiniciar el servidor, cuando se le solicite, presione F10 para acceder a Lifecycle Controller. Para ir a la página **Inventario de hardware**, seleccione **Configuración de hardware** > **Inventario de hardware**. En la página **Inventario de hardware** , haga clic en **Recopilar inventario del sistema al reinicio**.

El método **Actualizar desde archivo** permite actualizar el firmware de los componentes del servidor a través de archivos DUP almacenados en un sistema local. Es posible seleccionar componentes individuales para actualizar el firmware mediante los archivos DUP necesarios. Se puede actualizar una gran cantidad de componentes al mismo tiempo por medio de una tarjeta SD con un tamaño de memoria superior a 48 MB para almacenar los archivos DUP.

NOTA: Tenga en cuenta lo siguiente:

- Al seleccionar componentes individuales en el servidor para la actualización, asegúrese de que no existan dependencias entre los componentes seleccionados. De lo contrario, la selección de algunos componentes con dependencias en otros componentes para la actualización puede detener de forma abrupta el funcionamiento de ese servidor.
- Asegúrese de actualizar los componentes del servidor en el orden que se recomienda. De lo contrario, el proceso de actualización de firmware de los componentes puede no completarse correctamente.

  Los módulos de firmware de los componentes del servidor deben actualizarse siempre en el siguiente orden:

  – BIOS
  – Lifecycle Controller
  – iDRAC

El método Un solo clic para todas las actualizaciones blade o **Actualizar desde recurso compartido de red** permite actualizar el firmware de un componente del servidor mediante archivos DUP almacenados en un recurso compartido de red. Puede usar la función de actualización basada en Dell Repository Manager (DRM) para acceder a los archivos DUP almacenados en un recurso compartido de red y actualizar los componentes del servidor en una sola operación. Puede configurar un repositorio remoto personalizado de los DUP de firmware e imágenes binarias mediante Dell Repository Manager y compartirlo en el recurso compartido de red. Como alternativa, utilice Dell Repository Manager (DRM) para buscar las actualizaciones de firmware más recientes disponibles. Dell Repository Manager (DRM) garantiza que los sistemas Dell están actualizados con la última versión de BIOS, controladores, firmware y software. Puede buscar las actualizaciones más recientes disponibles en el sitio de asistencia (**support.dell.com**) para ver las plataformas admitidas según la marca y el modelo, o una etiqueta de servicio. Puede descargar las actualizaciones o crear un repositorio de los resultados de la búsqueda. Para obtener más información sobre el uso de DRM para buscar las actualizaciones de firmware más recientes, consulte Uso de Dell Repository Manager para buscar las actualizaciones más recientes en el sitio web de asistencia de Dell en Dell Tech Center. Para obtener información sobre cómo guardar el archivo de inventario que DRM utiliza como entrada para crear los repositorios, consulte Cómo guardar el informe de inventario del chasis mediante la interfaz web de la CMC

NOTA: El método Un solo clic para todas las actualizaciones blade presenta los siguientes beneficios:

- Permite actualizar todos los componentes de todos los servidores blade con una cantidad mínima de clics.
- Todas las actualizaciones se encuentran en paquetes en el directorio. De esta manera, no es necesario cargar de forma individual el firmware de cada uno de los componentes.
- Método más rápido y consistente para actualizar los componentes del servidor
- Permite mantener una imagen estándar con las versiones de actualización necesarias para los componentes del servidor que se pueden usar para actualizar varios servidores en una única operación.
- Es posible copiar los directorios de las actualizaciones con la herramienta Dell Server Update Utility (SUU), descargar DVD o crear y personalizar las versiones de actualización necesarias en Dell Repository Manager (DRM). No se necesita la versión más reciente de Dell Repository Manager para crear este directorio. Sin embargo, Dell Repository Manager versión 1.8 ofrece una opción para crear un repositorio (directorio de actualizaciones) basado en el inventario que se ha exportado de los servidores en el chasis. Para obtener información sobre la creación de un repositorio mediante Dell Repository Manager, consulte la *Dell Repository Manager Data Center Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Data Center versión 1.8)* y *Dell Repository Manager Business Client Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Business Client versión 1.8)* disponible en **dell.com/support/manuals**.

Lifecycle Controller ofrece compatibilidad para la actualización de módulos a través de iDRAC6. Se recomienda actualizar el firmware del CMC antes de actualizar los módulos de firmware de los componentes del servidor. Después de actualizar el firmware de la CMC, en la interfaz web de la CMC, es posible actualizar el firmware de los componentes del servidor en la página **Descripción general del chasis** > **Descripción general del servidor** > **Actualizar** > **Actualización de componentes del servidor**. Además, se recomienda seleccionar todos los módulos de los componentes de un servidor para actualizarlos de forma conjunta. Esto permite que Lifecycle Controller use algoritmos optimizados para actualizar el firmware y así, reducir la cantidad de reinicios.

Para actualizar el firmware de los componentes del servidor con la interfaz web de la CMC, haga clic en **Descripción general del chasis** > **Descripción general del servidor** > **Actualizar** > **Actualización de los componentes del servidor**.

Si el servidor no admite el servicio Lifecycle Controller, la sección **Inventario de firmware de componentes/dispositivos** muestra **No admitido**. Para los servidores de última generación, instale el firmware de Lifecycle Controller y actualice el firmware del iDRAC para activar el servicio Lifecycle Controller en el servidor. En servidores de generaciones anteriores, no se puede realizar esta actualización.

Generalmente, el firmware de Lifecycle Controller se instala mediante un paquete de instalación adecuado que se ejecuta en el sistema operativo del servidor. Para los servidores admitidos, está disponible una reparación especial o un paquete de instalación con una extensión de archivo **.usc**. Este archivo le permite instalar el firmware de Lifecycle Controller a través de la función de actualización de firmware disponible en la interfaz nativa del navegador web del iDRAC.

También puede instalar el firmware de Lifecycle Controller a través de un paquete de instalación apropiado que se ejecuta en el sistema operativo del servidor. Para obtener más información, consulte la *Dell Lifecycle Controller User's Guide* (Guía del usuario de Lifecycle Controller de Dell).

Si el servicio Lifecycle Controller está desactivado en el servidor, aparece la sección **Inventario de firmware de componentes y dispositivos**.

```
Lifecycle Controller may not be enabled.
```

Secuencia de actualización de componentes del servidor

En el caso de las actualizaciones de componentes individuales, es necesario actualizar las versiones de firmware de los componentes del servidor en la siguiente secuencia:

- iDRAC
- Lifecycle Controller
- Diagnósticos (opcional)
- Driver Packs del sistema operativo (opcional)
- BIOS
- NIC

- RAID
- Otros componentes

NOTA: Cuando se actualizan las versiones de firmware de todos los componentes del servidor a la vez, Lifecycle Controller controla la secuencia de actualización.

Habilitación de Lifecycle Controller

Es posible activar el servicio de Lifecycle Controller cuando se enciende un servidor:

- Para los servidores del iDRAC, en la consola de inicio, para acceder a **Configuración del sistema**, presione la tecla <F2>.
- En la página **Menú principal de Configuración del sistema**, vaya a **Configuración del iDRAC** > **Lifecycle Controller** y haga clic en **Activado**. Vaya a la página **Menú principal de Configuración del sistema** y haga clic en **Terminar** para guardar la configuración.

La cancelación de Servicios del sistema permite cancelar todos los trabajos programados pendientes y quitarlos de la cola.

Para obtener más información sobre Lifecycle Controller y los componentes del servidor admitidos y la administración de firmware de dispositivos, consulte:

- *Lifecycle Controller-Remote Services Quick Start Guide* (Guía de inicio rápido de servicios remotos de Lifecycle Controller).
- **delltechcenter.com/page/Lifecycle+Controller**.

La página **Actualización de los componentes del servidor** le permite actualizar diferentes componentes de firmware en el servidor. Para utilizar las funciones y características de esta página, es necesario tener:

- Para CMC: privilegios de **Server Administrator**.
- Para iDRAC: privilegio para **Configurar el iDRAC** y privilegio de **Inicio de sesión en el iDRAC**.

Si los privilegios no son suficientes, puede ver el inventario de firmware de los componentes y los dispositivos en el servidor. No puede seleccionar componentes ni dispositivos para una operación de Lifecycle Controller en el servidor.

Elección de tipo de actualización de firmware para los componentes del servidor mediante la interfaz web del CMC

Para seleccionar el tipo de actualización de componentes del servidor, escriba:

1 En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.

Aparecerá la página **Actualización de los componentes del servidor**.

2 En la sección **Seleccionar tipo de actualización**, seleccione el tipo de método de actualización necesario:
   - **Actualizar desde archivo**
   - **Actualizar desde recurso compartido de red**

Filtrado de componentes para actualizaciones de firmware

La información de todos los componentes y dispositivos en todos los servidores se recupera de una sola vez. Para administrar esta gran cantidad de información, Lifecycle Controller proporciona varios mecanismos de filtrado.

NOTA: Para usar esta función, debe tener una licencia Enterprise.

La sección **Filtro de actualización de componentes y dispositivos** de la página **Actualización de componentes del servidor** le permite filtrar la información según el componente y está disponible solamente con el modo de **Actualización mediante archivo**.

Estos filtros le permiten:

- Seleccionar una o más categorías de componentes o dispositivos para verlos más fácilmente.
- Comparar versiones de firmware de componentes y dispositivos en el servidor.
- Reducir la categoría de un componente o dispositivo particular en función de los tipos o modelos, filtrar automáticamente los componentes o dispositivos seleccionados.

NOTA: La función de filtro automático es importante al utilizar Dell Update Package (DUP). La programación de actualización de un DUP puede basarse en el tipo o modelo de un componente o dispositivo. El comportamiento de los filtros automáticos está diseñado para minimizar las decisiones de selección posteriores a una selección inicial.

A continuación se muestran algunos ejemplos en los que se han aplicado mecanismos de filtrado:

- Si se ha seleccionado el filtro BIOS, solamente se muestra el inventario de BIOS para todos los servidores. Si el conjunto de servidores consiste en un número de modelos de servidores y se selecciona un servidor para la actualización del BIOS, la lógica del filtro automático quita automáticamente todos los servidores que no coincidan con el modelo del servidor seleccionado. Esto garantiza que la selección de la imagen de actualización del firmware del BIOS (DUP) sea compatible con el modelo de servidor correcto.

  En ocasiones, la imagen de actualización del firmware del BIOS puede ser compatible con varios modelos de servidor. Estas optimizaciones se omiten si la compatibilidad ya no es vigente en el futuro.
- El filtro automático es importante para las actualizaciones de firmware de Controladoras de interfaz de red (NIC) y las Controladoras RAID. Estas categorías de dispositivos tienen distintos tipos y modelos. De forma similar, las imágenes de actualización del firmware (DUP) pueden estar disponibles en formularios optimizados en los que un solo DUP puede estar programado para actualizar varios tipos o modelos de dispositivos de una categoría determinada.

Filtrado de componentes para actualizaciones de firmware mediante la interfaz web del CMC

Para filtrar los dispositivos:

1. En el panel izquierdo, vaya a **Descripción general del servidor** y haga clic en **Actualizar**.
2. En la página **Actualización de los componentes del servidor**, en la sección **Filtro de actualización de componentes y dispositivos**, seleccione uno o varios de los siguientes:
   - **BIOS**
   - **iDRAC**
   - **Lifecycle Controller**
   - **Diagnósticos de 32 bits**
   - **Driver Pack del sistema operativo**
   - **Controladora de la red I/F**
   - **Controladora RAID**

   La sección **Filtro para actualizar componentes y dispositivos** se visualiza solamente con el modo de **Actualización mediante archivo** al actualizar el firmware.

   La sección **Inventario de firmware** muestra únicamente los componentes o dispositivos asociados en todos los servidores presentes en el chasis. Después de seleccionar un elemento del menú desplegable, solo se muestran los componentes o dispositivos asociados a los que están la lista.

   Después de que aparezca el conjunto de componentes y dispositivos filtrado en la sección de inventario, el filtrado puede continuar si el componente o dispositivo se selecciona para una actualización. Por ejemplo, si se selecciona el filtro del BIOS, la sección de inventario muestra todos los servidores solamente con su componente de BIOS. Si se selecciona un componente de BIOS en uno de los servidores, el inventario se filtra aún más para mostrar los servidores que coinciden con el nombre de modelo del servidor seleccionado.

   Si no se selecciona ningún filtro y se selecciona un componente o dispositivo para su actualización en la sección de inventario, el filtro relacionado con esa selección se activa automáticamente. Se pueden generar otros filtros en los que la sección de inventario muestra

todos los servidores que coinciden con el componente seleccionado según el modelo, el tipo u otra forma de identidad. Por ejemplo, si se selecciona un componente de BIOS en uno de los servidores para su actualización, el filtro se aplica en el BIOS automáticamente y la sección de inventario muestra los servidores que coinciden con el nombre de modelo del servidor seleccionado.

Filtrado de componentes para actualizaciones de firmware mediante RACADM

Para filtrar los componentes para actualizaciones de firmware mediante RACADM, ejecute el comando **getversion**:

```
racadm getversion -l [-m <module>] [-f <filter>]
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en **dell.com/support/manuals**.

Visualización del inventario de firmware

Es posible ver el resumen de las versiones de firmware para todos los componentes y los dispositivos de todos los servidores actualmente presentes en el chasis junto con su estado.

NOTA: Para usar esta función, debe tener una licencia Enterprise.

Visualización del inventario de firmware mediante la interfaz web del CMC

Para ver el inventario de firmware:

1. En el panel izquierdo, haga clic en **Descripción general del servidor** y, a continuación, haga clic en **Actualizar**.
2. En la página **Actualización de los componentes del servidor**, visualice los detalles del inventario de firmware en la sección **Inventario de firmware de componentes/dispositivos**. En esta página, puede ver la siguiente información:
   - Los servidores que actualmente no admiten el servicio de Lifecycle Controller se detallan como **No admitido**. Se ofrece un hipervínculo a una página alternativa donde es posible actualizar de forma directa únicamente el firmware del iDRAC. Esta página solo admite la actualización de firmware del iDRAC y no de otro componente o dispositivo en el servidor. La actualización de firmware del iDRAC no depende del servicio de Lifecycle Controller.
   - Si el servidor aparece como **No listo**, eso indica que cuando se recuperó el inventario de firmware, el iDRAC del servidor aún se estaba inicializando. Espere hasta que iDRAC esté completamente operativo y actualice la página para recuperar el inventario de firmware.
   - Si el inventario de componentes y dispositivos no refleja lo que está físicamente instalado en el servidor, invoque Lifecycle Controller cuando el servidor esté en proceso de inicio. Esto ayuda a actualizar la información de los componentes y dispositivos integrados y permite verificar los componentes y los dispositivos instalados actualmente. El inventario no refleja la información de componentes y dispositivos con precisión cuando:
     - Se actualiza el firmware del iDRAC del servidor con una funcionalidad recién introducida de Lifecycle Controller para la administración del servidor.
     - Se insertan nuevos dispositivos en el servidor.

     Para automatizar esta acción, la utilidad de configuración de iDRAC proporciona una opción a la que se puede acceder a través de la consola de inicio:

     1. Para los servidores del iDRAC, en la consola de inicio, para acceder a **Configuración del sistema**, presione <F2>.
     2. En la página **Menú principal de la configuración del sistema**, haga clic en **Configuración del iDRAC** > **Recopilar inventario del sistema al reinicio**, seleccione **Activado**, regrese a la página **Menú principal de la configuración del sistema** y haga clic en **Finalizar** para guardar la configuración.

- Se encuentran disponibles opciones para las diversas operaciones de Lifecycle Controller como Actualizar, Revertir, Reinstalar y Eliminación de trabajos. Solo se puede realizar un tipo de operación por vez. Los componentes y los dispositivos no admitidos pueden aparecer como parte del inventario, pero no permiten las operaciones de Lifecycle Controller.

En la siguiente tabla se muestra la información de los componentes y los dispositivos en el servidor:

Tabla 12. Información sobre componentes y dispositivos

Campo	Descripción
Ranura	Muestra la ranura que ocupa el servidor en el chasis. Los números de ranura son identificaciones secuenciales, de 1 a 4 (para las cuatro ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis. Si hay menos de 4 servidores que ocupan ranuras, solamente se muestran las ranuras ocupadas por servidores.
Nombre	Muestra el nombre del servidor en cada ranura.
Modelo	Muestra el modelo del servidor.
Componente/ Dispositivo	Muestra una descripción del componente o dispositivo en el servidor. Si el ancho de la columna es demasiado estrecho, la herramienta de pasar el cursor permite ver la descripción.
Versión actual	Muestra la versión actual del componente o del dispositivo en el servidor.
Versión de reversión	Muestra la versión de reversión del componente o del dispositivo en el servidor.
Estado del trabajo	Muestra el estado del trabajo de las operaciones programadas en el servidor. El estado del trabajo se actualiza continuamente de forma dinámica. Si se detecta la compleción de un trabajo con el estado completado, las versiones de firmware de los componentes y dispositivos en ese servidor se actualizan automáticamente cuando se realiza un cambio de versión de firmware en alguno de los componentes o dispositivos. También se muestra un ícono de información junto al estado actual para ofrecer información adicional sobre el estado actual del trabajo. Al hacer clic en el ícono o pasar el cursor sobre el mismo, se puede ver esta información.
Actualizar	Haga clic en seleccionar el componente o dispositivo para la actualización de firmware del servidor.

Visualización del inventario de firmware mediante RACADM

Para visualizar el inventario de firmware mediante RACADM, use el comando `getversion`:

```
racadm getversion -l [-m <module>] [-f <filter>]
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Cómo guardar el informe de inventario del chasis mediante la interfaz web del CMC

Para guardar el informe de inventario del chasis:

1 En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.

Aparecerá la página **Actualización de los componentes del servidor**.

2 Haga clic en **Guardar informe de inventario**.

El archivo *Inventory.xml* se guarda en un sistema externo.

NOTA: La aplicación Dell Repository Manager utiliza el archivo *Inventory.xml* como entrada para crear un repositorio de actualizaciones para todos los servidores blade disponibles en el chasis. Este repositorio se puede exportar posteriormente a un recurso compartido de red. El modo Actualizar desde recurso compartido de red de actualización del firmware usa este recurso compartido de red para actualizar los componentes de todos los servidores. CSIOR debe estar activado en los servidores individuales y se debe guardar el informe de inventario del chasis cada vez que se produzca un cambio en la configuración de hardware y software del chasis.

Configuración de un recurso compartido de red mediante la interfaz web del CMC

Para configurar o editar las credenciales o la ubicación de un recurso compartido de red:

1 En la interfaz web de CMC, en el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Recurso compartido de red**.

Se mostrará la sección **Editar recurso compartido de red**.

NOTA: Cuando tenga la misma carpeta para chasis, servidor y perfil de identidad de inicio, es posible que experimente problemas de rendimiento si hay más de 100 perfiles.

2 En la sección **Editar recurso compartido de red**, configure los siguientes valores según sea necesario:

- Protocolo
- Dirección IP o nombre del host
- Nombre del recurso compartido
- Carpeta de actualización
- Nombre de archivo (opcional)

NOTA: Nombre de archivo es opcional solamente cuando el nombre de archivo de catálogo predeterminado es catalog.xml. Si el nombre de archivo de catálogo se cambia, se debe ingresar el nombre nuevo en este campo.

- Carpeta de perfil
- Nombre de dominio
- Nombre del usuario
- Contraseña
- Versión de SMB

NOTA: La opción versión SMB solo está disponible si el tipo de protocolo es CIFS.

NOTA: Si está utilizando un CIFS que está registrado con un dominio y accede al CIFS mediante la IP con las credenciales de usuario local de CIFS, es obligatorio que ingrese el nombre de host o la IP de host en el campo Nombre de dominio.

Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

3 Haga clic en **Probar directorio** para verificar si se puede leer y escribir en los directorios.

4 Haga clic en **Probar conexión de red** para verificar si se puede acceder a la ubicación del recurso compartido de red.

Cuando aplica una versión SMB, el recurso compartido de red existente se desinstala y se vuelve a instalar cuando hace clic en **Probar conexión de red** o navega en otras páginas de GUI.

5 Haga clic en **Aplicar** para aplicar los cambios en las propiedades del recurso compartido de red.

NOTA:

Haga clic en **Atrás** para volver a la página **Actualización de componentes del servidor**.

Operaciones de Lifecycle Controller

NOTA: Para usar esta función, debe tener una licencia Enterprise.

Es posible realizar operaciones de Lifecycle Controller tales como:

- Vuelva a instalarla
- Revertir
- Actualizar
- Eliminar trabajos

Solo se puede realizar un tipo de operación por vez. Los componentes y los dispositivos no admitidos pueden aparecer como parte del inventario, pero no permiten las operaciones de Lifecycle Controller.

Para realizar operaciones de Lifecycle Controller, debe contar con lo siguiente:

- Para CMC: privilegios de Server Administrator.
- Para iDRAC: privilegio para Configurar el iDRAC y privilegio de Inicio de sesión en el iDRAC.

La operación programada de Lifecycle Controller en un servidor puede tardar entre 10 y 15 minutos en completarse. El proceso implica varios reinicios del servidor mientras se instala el firmware, como también una fase de verificación del firmware. Podrá ver el progreso de este proceso en la consola del servidor. Si se necesita actualizar varios componentes o dispositivos en un servidor, puede agrupar todas las actualizaciones en una operación programada y minimizar la cantidad de reinicios necesarios.

En ocasiones, cuando una operación está en proceso de enviarse para su programación a través de otra sesión o contexto, se intenta realizar otra operación. En este caso, aparecerá un mensaje de confirmación donde se explicará la situación y se indicará que la operación no debe enviarse. Espere a que la operación en proceso se complete y vuelva a intentar enviar la operación.

No navegue fuera de la página una vez que haya enviado una operación para su programación. Si lo intenta, aparecerá un mensaje de confirmación en el que se puede cancelar la navegación. De lo contrario, la operación se interrumpirá. Una interrupción, especialmente durante una operación de actualización, puede finalizar la carga del archivo de imagen del firmware antes de tiempo. Después de enviar una operación para su programación, asegúrese de aceptar el mensaje de confirmación que indica que la operación se ha programado correctamente.

Reinstalación del firmware de los componentes del servidor

Es posible reinstalar la imagen del firmware instalado anteriormente para los componentes o dispositivos seleccionados en uno o varios servidores. La imagen de firmware está disponible dentro de Lifecycle Controller.

Reinstalación del firmware de los componentes del servidor mediante la interfaz web

Para volver a instalar el firmware de los componentes de un servidor:

1. En el panel izquierdo, haga clic en **Descripción general del servidor** > **Actualizar**.
2. En la página **Actualización de componentes del servidor**, en la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**.
3. En la columna **Versión actual**, seleccione la opción correspondiente al componente o dispositivo para el cual desea volver a instalar el firmware.
4. Seleccione una de las siguientes opciones:
   - **Reiniciar ahora**: reinicia el servidor inmediatamente.
   - **En el próximo reinicio**: se reinicia manualmente el servidor en otro momento.
5. Haga clic en **Reinstalar**. La versión del firmware se vuelve a instalar para el componente o dispositivo seleccionado.

Reversión del firmware de los componentes del servidor

Es posible instalar la imagen del firmware instalado anteriormente para los componentes o dispositivos seleccionados en uno o varios servidores. La imagen de firmware está disponible dentro de Lifecycle Controller para una operación de reversión. La disponibilidad está

sujeta a la lógica de compatibilidad con la versión de Lifecycle Controller. También se presupone que Lifecycle Controller ha facilitado la actualización anterior.

NOTA: Para usar esta función, debe tener una licencia Enterprise.

Reversión del firmware de los componentes del servidor mediante la interfaz web del CMC

Para revertir la versión de firmware de los componentes del servidor a una versión anterior:

1 En el panel izquierdo, haga clic en **Descripción general del servidor→ Actualizar**.
2 En la página **Actualización de componentes del servidor**, en la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**.
3 En la columna **Revertir versión**, seleccione la casilla del componente o dispositivo para el cual desea revertir el firmware.
4 Seleccione una de las siguientes opciones:
   - **Reiniciar ahora**: reinicia el servidor inmediatamente.
   - **En el próximo reinicio**: se reinicia manualmente el servidor en otro momento.
5 Haga clic en **Rollback (Revertir)**. La versión del firmware previamente instalada se vuelve a instalar para el componente o dispositivo seleccionado.

Actualización de firmware de los componentes del servidor

Es posible instalar la siguiente versión de la imagen de firmware para los componentes o dispositivos seleccionados en uno o varios servidores. La imagen de firmware está disponible dentro de Lifecycle Controller para una operación de reversión. Para usar esta función, debe tener una licencia Enterprise.

NOTA: Para realizar una actualización de firmware de los Driver Pack en el SO y el iDRAC, asegúrese de que la función Almacenamiento extendido esté activada.

Se recomienda borrar la cola de trabajos antes de iniciar una actualización de firmware de los componentes en el servidor. Una lista de todos los trabajos en los servidores está disponible en la página **Trabajos de Lifecycle Controller**. Esta página permite borrar uno o varios trabajos, o depurar todos los trabajos en el servidor.

Las actualizaciones del BIOS son específicas del modelo de servidor. A veces, aunque se haya seleccionado un solo dispositivo de la controladora de interfaz de red (NIC) para la actualización de firmware en el servidor, la actualización puede aplicarse a todos los dispositivos NIC en el servidor. Este comportamiento es propio de la funcionalidad de Lifecycle Controller y, particularmente, de la programación en Dell Update Packages (DUP). Actualmente, se admiten Dell Update Packages (DUP) de un tamaño inferior a 48 MB.

Si el tamaño de la imagen en el archivo de actualización es mayor, el estado del trabajo indica que se ha producido una falla en la descarga. Si se intenta actualizar varios componentes en un servidor, el tamaño combinado de todos los archivos de actualización del firmware también podrá superar los 48 MB. En dicho caso, las actualizaciones de uno de los componentes fallan ya que se trunca su archivo de actualización. Para actualizar varios componentes en un servidor, se recomienda actualizar primero los componentes de Lifecycle Controller y de Diagnósticos de 32 bits juntos. Estos componentes no necesitan que se reinicie el servidor y se completan relativamente rápido. Luego, los demás componentes pueden actualizarse juntos.

Todas las actualizaciones de Lifecycle Controller se programan para ejecutarse inmediatamente. Sin embargo, en ocasiones, los servicios del sistema pueden retrasar esta ejecución. En dichas situaciones, la actualización falla como consecuencia de que el recurso compartido remoto que se aloja en la CMC ya no está disponible.

Actualización de firmware de los componentes del servidor desde un archivo mediante la interfaz web del CMC

Para actualizar la versión de firmware de los componentes de un servidor a la siguiente versión mediante el modo **Actualizar desde archivo**:

1 En la interfaz web de la CMC, en el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.

Aparecerá la página **Actualización de los componentes del servidor**.

2 En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**. Para obtener más información, consulte Elección del tipo de actualización de firmware para los componentes del servidor mediante la interfaz web de la CMC.

3 En la sección **Filtro para actualizar componentes y dispositivos**, filtre el componente o el dispositivo (opcional). Para obtener más información, consulte Filtrado de componentes para actualizaciones de firmware mediante la interfaz web de la CMC.

4 En la columna **Actualizar**, seleccione las casillas de verificación del componente o dispositivo para el cual desea actualizar el firmware a la próxima versión. Use el acceso directo de la tecla CRTL para seleccionar un tipo de componente o dispositivo y actualizarlo en todos los servidores aplicables. Si mantiene presionada la tecla CRTL, todos los componentes se resaltarán en amarillo. Al mismo tiempo que mantiene presionada la tecla CRTL, seleccione el componente o dispositivo requerido. Para ello, active la casilla de verificación asociada en la columna **Actualizar**.

Se mostrará una segunda tabla que enumera los tipos de componentes o dispositivos seleccionados y un selector para el archivo de imagen de firmware. En cada tipo de componente, se mostrará un selector para el archivo de imagen de firmware.

Existen pocos dispositivos, como las Controladoras de interfaz de red (NIC) y las controladoras RAID, que contengan muchos tipos y modelos. La lógica de selección de actualizaciones filtra automáticamente el modelo o el tipo de dispositivo relevante en función de los dispositivos seleccionados en un principio. El principal motivo de este comportamiento de filtrado automático es que se puede especificar un solo archivo de imagen de firmware para la categoría.

NOTA: El límite de tamaño de la actualización para un solo DUP o varios DUP combinados se puede ignorar si la función Almacenamiento extendido está instalada y activada. Para obtener información sobre cómo activar el almacenamiento extendido, consulte Configuración de la tarjeta de almacenamiento extendido de la CMC.

5 Especifica el archivo de imagen del firmware para los componentes o dispositivos seleccionados. Este es un archivo Dell Update Package (DUP) para Microsoft Windows.

6 Seleccione una de las siguientes opciones:

- **Reiniciar ahora**: se reinicia el servidor y se aplica la actualización de firmware inmediatamente.
- **En el siguiente reinicio**: se reinicia el servidor de forma manual en otro momento. La actualización de firmware se aplica después del siguiente reinicio.

NOTA: Este paso no es válido para las actualizaciones de firmware en Lifecycle Controller y Diagnósticos de 32 bits. No se requiere el reinicio del servidor para estos componentes.

7 Haga clic en **Update** (Actualizar). Se actualizará la versión de firmware para el componente o dispositivo seleccionado.

Actualización con un solo clic de componentes del servidor mediante recurso compartido de red

La actualización de componentes de servidores desde un recurso compartido de red mediante Dell Repository Manager y la integración del chasis Dell PowerEdge VRTX simplifica la actualización mediante el paquete de firmware personalizado para que pueda implementar de manera más fácil y rápida. Actualizar desde un recurso compartido de red proporciona flexibilidad para actualizar todos los componentes del servidor de 12.a generación al mismo tiempo con un solo catálogo desde un NFS o CIFS.

Este método proporciona una forma rápida y sencilla de crear un repositorio personalizado para los sistemas conectados con los que cuenta mediante Dell Repository Manager y el archivo de inventario del chasis exportado mediante la interfaz web de la CMC. DRM le permite

crear un repositorio totalmente personalizado que solo incluye los paquetes de actualización para la configuración específica del sistema. También puede crear repositorios que contengan actualizaciones solo para dispositivos desactualizados o un repositorio de línea de base que contenga actualizaciones para todos los dispositivos. También puede crear paquetes de actualización para Linux o Windows basados en el modo de actualización requerido. DRM le permite guardar el repositorio en un recurso compartido CIFS o NFS. La interfaz web de la CMC le permite configurar las credenciales y los detalles de la ubicación del recurso compartido. Mediante la interfaz web de la CMC, puede realizar la actualización de los componentes del servidor para uno o varios servidores.

Prerrequisitos para utilizar el modo de actualización de un recurso compartido de red

Los siguientes prerrequisitos son necesarios para actualizar el firmware de los componentes del servidor mediante el modo del recurso compartido de red:

- Los servidores deben pertenecer a la 12.ª generación o a generaciones posteriores y debe tener la licencia de iDRAC Enterprise.
- La versión del CMC debe ser 2.0 o posterior.
- Lifecycle Controller debe estar activado en los servidores.
- La versión 1.50.50 o posterior del iDRAC debe estar disponible en los servidores de 12.ª generación.
- Dell Repository Manager 1.8 o posterior debe estar instalado en el sistema.
- Debe tener privilegios de administrador de lal CMC.

Actualización de firmware de los componentes del servidor desde un recurso compartido de red mediante la interfaz web del CMC

Para actualizar la versión de firmware de los componentes de un servidor a la siguiente versión mediante el modo **Actualizar desde recurso compartido de red**:

1 En la interfaz web del CMC, en el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.

Aparecerá la página **Actualización de los componentes del servidor**.

2 En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde recurso compartido de red**. Para obtener más información, consulte la sección Elección de tipo de actualización de firmware de los componentes del servidor.

3 Si el recurso compartido de red no está conectado, configure el recurso compartido de red del chasis. Para configurar o editar los detalles del recurso compartido de red, en la tabla Propiedades del recurso compartido de red, haga clic en **Editar**. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web del CMC.

4 Haga clic en **Guardar informe de inventario** para exportar el archivo de inventario del chasis que contiene los detalles de los componentes y el firmware.

El archivo *Inventory.xml* se guarda en un sistema externo. Dell Repository Manager utiliza el archivo *inventory.xml* para crear conjuntos de paquetes personalizados de actualizaciones. Este repositorio se guarda en el recurso compartido de CIFS o NFS configurado por la CMC. Para obtener información sobre la creación de un repositorio mediante Dell Repository Manager, consulte la *Dell Repository Manager Data Center Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Data Center versión 1.8)* y *Dell Repository Manager Business Client Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Business Client versión 1.8)* disponible en **dell.com/support/manuals**.

5 Haga clic en **Buscar actualizaciones** para ver las actualizaciones de firmware disponibles en el recurso compartido de red.

En la sección **Inventario de firmware de componentes y dispositivos**, se muestran las versiones de firmware actuales de los componentes y los dispositivos de todos los servidores presentes en el chasis y las versiones de firmware de los paquetes de actualización Dell disponibles en el recurso compartido de red.

NOTA: Haga clic en Contraer en una ranura para contraer los detalles del firmware de componentes y dispositivos de la ranura específica. De forma alternativa, para ver todos los detalles de nuevo, haga clic en Expandir.

6 En la sección **Inventario de firmware de componentes y dispositivos**, seleccione la casilla junto a **Seleccionar/Deseleccionar todo** para seleccionar todos los servidores compatibles. De forma alternativa, seleccione la casilla junto al servidor en el que desea actualizar el firmware de los componentes. No se pueden seleccionar componentes individuales para el servidor.

7 Seleccione una de las siguientes opciones para especificar si es necesario reiniciar el sistema después de programar las actualizaciones:

- Reiniciar ahora: Se programan las actualizaciones, se reinicia el servidor y, a continuación, se aplican inmediatamente las actualizaciones a los componentes del servidor.
- En el siguiente reinicio: Las actualizaciones se programan, pero solo se aplican después del siguiente reinicio del servidor.

8 Haga clic en **Actualizar** para programar las actualizaciones de firmware en los componentes disponibles de los servidores seleccionados.

Según el tipo de actualizaciones incluidas, se mostrará un mensaje donde se le solicitará confirmar si desea continuar.

9 Haga clic en **Aceptar** para continuar y completar la programación de las actualizaciones de firmware en los servidores seleccionados. Nota:

NOTA: La columna Estado de trabajo muestra el estado de las operaciones programadas en el servidor. El estado de trabajo se actualiza de forma dinámica.

Versiones de firmware admitidas para la actualización de componentes del servidor

La siguiente sección proporciona la Actualización de componentes del servidor para la CMC.

En la siguiente tabla se indican las versiones de firmware admitidas para los componentes del servidor en una situación en la que la versión existente de firmware del CMC es 3.1 y los componentes del servidor se actualizan de la versión N-1 a la versión N.

NOTA: La actualización de firmware de los componentes del servidor de la versión N-1 a la versión N se realiza correctamente cuando el firmware de la CMC es 2.0 o posterior en todos los servidores de 12.º, 13.º y 14.º generación que se mencionan en la siguiente tabla.

Tabla 13. Versiones admitidas de los componentes del servidor para la actualización de componentes del servidor a la versión N

Plataforma	Componente del servidor	Versión anterior de cada componente (versión N-1)	Versión actualizada de cada componente (versión N)
M520	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnóstico	4231A0	4247A1
	BIOS	2.4.2	2.6.1
	NIC	19.2.0	20.00.00.13
M620	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnóstico	4231A0	4247A1
	BIOS	2.5.4	2.6.1
M820	iDRAC	2.52.52.52	2.60.60.60

Plataforma	Componente del servidor	Versión anterior de cada componente (versión N-1)	Versión actualizada de cada componente (versión N)
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnóstico	4231A0	4247A1
	BIOS	2.6.1	2.6.1
M630	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnóstico	4239.44	4239A36
	BIOS	2.6.0	2.7.1
M830	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnóstico	4239.44	4239A36
	BIOS	2.5.4	2.7.1
M640	iDRAC	3.15.15.15	3.21.21.21
	Lifecycle Controller	3.15.15.15	3.21.21.21
	Diagnóstico	4301A13	4301A13
	BIOS	1.3.7	1.4.8

Eliminación de trabajos programados sobre el firmware de los componentes del servidor

NOTA: Para usar esta función, debe tener una licencia Enterprise.

Es posible eliminar trabajos programados para componentes o dispositivos seleccionados en uno o varios servidores.

Eliminación de trabajos programados sobre el firmware de los componentes del servidor mediante la interfaz web

Para eliminar trabajos programados sobre el firmware de los componentes del servidor:

1. En el panel izquierdo, haga clic en **Descripción general del servidor** y, a continuación, haga clic en **Actualizar**.
2. En la página **Actualización de los componentes del servidor**, filtre el componente o dispositivo (opcional).
3. En la columna **Estado de trabajo**, si se muestra una casilla junto al estado del trabajo, significa que existe un trabajo de Lifecycle Controller en progreso y se encuentra en el estado indicado. Se puede seleccionar para una operación de eliminación de trabajos.
4. Haga clic en **Eliminar trabajo**. Se borran los trabajos para los componentes o dispositivos seleccionados.

Actualización de los componentes de almacenamiento mediante la interfaz web del CMC

Asegúrese de descargar los DUP para los componentes de almacenamiento requeridos.
Para actualizar los componentes de almacenamiento:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Actualizar**.

2 En la página **Actualización de componentes de almacenamiento**, haga clic en **Examinar**.

Aparece el cuadro de diálogo **Seleccionar para cargar archivo**

3 Navegue hasta la ubicación en la que se descargó y guardó el archivo de DUP necesario desde el sitio de asistencia de Dell y seleccione el archivo de DUP y haga clic en **Abrir**.

El nombre y la ruta de acceso del archivo de DUP aparecen en el campo **Examinar**.

4 Haga clic en **Cargar**.

El DUP está cargado en el CMC. La sección **Actualización de los componentes de almacenamiento** muestra solo los componentes que son compatibles con el archivo de DUP descargado. Aparecen la versión actual, la versión más reciente disponible y la casilla de verificación **Actualizar** para los componentes.

5 Seleccione las casillas de verificación **Actualizar** que corresponda para los componentes necesarios.

6 Haga clic en **Update** (Actualizar).

Se inicia la acción de actualización del firmware para los componentes seleccionados. El progreso aparece en la columna **Actualizar**

Una vez finalizada la acción, aparecerá el mensaje correspondiente para indicar la finalización o la falla de la actualización del firmware.

NOTA:

- Los servidores deben apagarse antes de actualizar el firmware.
- El componente actualiza otros componentes correspondientes del sistema de manera similar. Por ejemplo, las SPERC actualizan de manera similar a las SPERC existentes y las EMM actualizan de manera similar a las EMM integradas.
- Haga clic en el  para ver la unidad de disco duro de los diferentes gabinetes.

Recuperación de firmware del iDRAC mediante el CMC

El firmware del iDRAC se actualiza normalmente a través de las interfaces del iDRAC, como la interfaz web del iDRAC, la interfaz de línea de comandos SM-CLP o los paquetes de actualización específicos del sistema operativo descargados desde **dell.com/support**. Para obtener más información, consulte *iDRAC User's Guide* (Guía del usuario del iDRAC).

Las primeras generaciones de servidores pueden recuperar el firmware dañado mediante el nuevo proceso de actualización de firmware del iDRAC. Cuando la CMC detecta el firmware dañado del iDRAC, indica el servidor en la página **Actualización del firmware**. Complete las tareas mencionadas en la sección Actualización de firmware del iDRAC del servidor.

5

Visualización de información del chasis y supervisión de la condición de los componentes y del chasis

Es posible ver información y supervisar la condición de los siguientes elementos:

- CMC activos y en espera
- Todos los servidores y los servidores individuales
- Módulo de E/S
- Ventiladores
- Unidades de suministro de energía (PSU)
- Sensores de temperatura
- Unidades de discos duros
- El conjunto de LCD
- Controladoras de almacenamiento
- Dispositivos PCIe

NOTA: La condición de componentes externos influye en la condición general del componente de almacenamiento con estado de almacenamiento y componentes de almacenamiento integrado existentes en VRTX. Esto indica que los componentes externos no afectarán la condición de ningún componente en el chasis.

Temas:

Visualización de los resúmenes de los componentes y el chasis

Al iniciar sesión en la interfaz web de la CMC, la página **Condición del chasis** muestra la condición del chasis y de sus componentes. Muestra una vista gráfica del chasis y de sus componentes. Se actualiza de manera dinámica y las superposiciones de subgráficos de componentes y sugerencias de texto se cambian automáticamente para reflejar el estado actual.

Para ver la condición del chasis, haga clic en **Descripción general del chasis**. El sistema muestra la condición general del chasis, las CMC activas y en estado de espera, los módulos de los servidores, el módulo de E/S (IOM), los ventiladores y sopladores, las unidades de suministro de energía (PSU), el conjunto del LCD, la controladora de almacenamiento y los dispositivos PCIe. Cuando hace clic en un componente, aparece información detallada sobre cada uno. Además, se muestran los sucesos más recientes en el registro de hardware de la CMC. Para obtener más información, consulte la *Ayuda en línea*.

NOTA: Después de ejecutar un ciclo de apagado y encendido del chasis o un comando "racreset", se eliminarán las alertas de una unidad física que se encuentre en estado "sin conexión".

Si el chasis se ha configurado como el chasis principal del grupo, se muestra la página **Condición del grupo** después del inicio de sesión. Se muestra la información de nivel del chasis y las alertas. Se mostrarán todas las alertas, activas, críticas y no críticas.

Gráficos del chasis

El chasis se representa mediante las vistas frontal y posterior de las imágenes en la parte superior e inferior, respectivamente. Los servidores, DVD, HDD, KVM y LCD se muestran en la vista frontal y los componentes restantes se muestran en la vista posterior. El color azul dominante indica la selección del componente y se controla haciendo clic en la imagen del componente requerido. Cuando un componente está presente en el chasis, se muestra un ícono del tipo de componente en los gráficos, en la posición (ranura) en donde se ha instalado el componente. Las posiciones vacías se muestran con un fondo gris. El ícono del componente indica visualmente su estado. Otros componentes muestran íconos que representan visualmente el componente físico. Al pasar el cursor sobre un componente, aparece información sobre herramientas con información adicional acerca de ese componente.

Tabla 14. Estados del icono del servidor en sistemas de 13.ª generación

Icono	Descripción
	El servidor está presente, está encendido y funciona con normalidad.
	Hay un servidor presente, pero está apagado.
	Hay un servidor presente, pero indica un error no crítico.
	Hay un servidor presente, pero indica un error crítico.
	El servidor no está presente.

Tabla 15. Estados del icono del servidor en sistemas de 14.ª generación

Icono	Descripción
	El servidor está presente, está encendido y funciona con normalidad.
	Hay un servidor presente, pero está apagado.

Icono	Descripción
	Hay un servidor presente, pero indica un error no crítico.
	Un servidor está presente pero informa un error crítico.
	Un servidor no está presente.

NOTA: De manera predeterminada, los iconos de estado del servidor en los sistemas PowerEdge de 13.ª generación de Dell se muestran si inserta un servidor PowerEdge de 14.ª generación cuando el chasis está apagado.

Información del componente seleccionado

La información del componente seleccionado se muestra en tres secciones independientes:

- Condición, rendimiento y propiedades: muestra los sucesos activos, críticos y no críticos como aparecen en los registros de hardware y los datos de rendimiento que varían con el tiempo.
- Propiedades: muestra las propiedades de los componentes que no varían con el tiempo y solo cambian cada tanto.
- Vínculos de acceso rápido: proporciona vínculos para navegar hasta las páginas con mayor acceso y hasta las acciones realizadas con mayor frecuencia. Esta sección solo muestra vínculos aplicables al componente seleccionado.

La siguiente tabla enumera las propiedades de los componentes y la información que se muestran en la página **Estado del chasis** en la interfaz web.

NOTA: En Administración de chasis múltiples (MCM), no se muestran todos los vínculos de acceso rápido asociados con los servidores.

Tabla 16. Propiedades de los componentes

Componente	Propiedades de condición y rendimiento	Propiedades	Vínculos de acceso rápido
Conjunto de LCD	• Condición de LCD • Condición del chasis	• Botón de encendido del chasis • Bloquear panel de control de LCD • Idioma de LCD • Orientación de LCD	Configuración del panel frontal

CMC activas y en espera	• Modo de redundancia • Dirección MAC • IPv4 • IPv6	• Firmware • Firmware en espera • Última actualización • Hardware	• Estado de la CMC • Sistema de red • Actualización del firmware
Todos los servidores y servidores individuales	• Estado de la alimentación • Consumo de alimentación • Condición • Energía asignada • Temperatura	• Nombre • Modelo • Etiqueta de servicio • Nombre del host • iDRAC • CPLD • BIOS • Sistema operativo • Información de la CPU • Memoria total del sistema	• Server Status (Estado del servidor) • Iniciar la consola remota • Iniciar la interfaz gráfica de usuario del iDRAC • Apagar el servidor • Apagado ordenado • Recurso compartido de archivos remotos • Implementar red del iDRAC • Actualización de componentes del servidor **NOTA: Los vínculos rápidos Apagar servidor y Apagado ordenado se muestran solamente si el estado de alimentación del servidor es Encendido. Si el estado de alimentación del servidor es Apagado, se muestra el vínculo de acceso rápido Encender servidor.**
Ranura de KVM	Condición	• KVM asignado • Ranura 1: USB/video del panel frontal activado • Ranura 2: USB/video del panel frontal activado • Ranura 3: USB/video del panel frontal activado • Ranura 4: USB/video del panel frontal activado	Configuración del panel frontal
Ranura de DVD	• Condición • Estado de la alimentación	• DVD asignado • Ranura 1: DVD activado • Ranura 2: DVD activado • Ranura 3: DVD activado • Ranura 4: DVD activado	Configuración del panel frontal
Ranura de disco	• Condición • Estado	• Modelo • Número de serie • Estado de la alimentación • Versión del firmware • Tamaño	• Estado del disco físico • Configuración del disco físico • Ver controladora para este disco físico • Ver discos virtuales para este disco físico

		• Tipo	
Unidades del sistema de alimentación	Estado de la alimentación	Capacidad	• Estado del suministro de energía • Consumo de alimentación • Presupuesto del sistema
Dispositivos PCIe	• Instalada • Asignada	• Modelo • Asignación de ranura del servidor • Id. de vendedor • Id. de dispositivo • Tipo de ranura • Alimentación asignada • Red Fabric • Estado de la alimentación	• Estado de PCIe • Configuración de PCIe
Ventiladores	• Velocidad • PWM (% del máximo) • Desplazamiento del ventilador	• Umbral de aviso • Umbral crítico	• Estado de los ventiladores • Configuración del ventilador
Ventilación	• Velocidad • PWM (% del máximo) • Modo de enfriamiento mejorado	• Umbral de aviso • Umbral crítico	• Estado de los ventiladores • Configuración del ventilador
Ranura SPERC	• Instalada • Asignada	• Modelo • Asignación de ranura del servidor • Id. de vendedor • Id. de dispositivo • Tipo de ranura • Alimentación asignada • Red Fabric • Estado de la alimentación	• Estado de la controladora • Configuración de la controladora
Ranura de la tarjeta PERC 8 compartida externa	• Instalada • Asignada	• Modelo • Asignación de ranura del servidor • Id. de vendedor • Id. de dispositivo • Tipo de ranura • Alimentación asignada • Red Fabric • Estado de la alimentación	• Estado de las ranuras de PCIe • Configuración de PCIe
Ranura del módulo de E/S	• Estado de la alimentación • Rol	• Modelo • Etiqueta de servicio	Estado del módulo de E/S Iniciar interfaz gráfica de usuario del módulo de E/S

Visualización del nombre de modelo del servidor y de la etiqueta de servicio

Es posible ver el nombre de modelo y la etiqueta de servicio de cada servidor en forma instantánea mediante los pasos siguientes:

1 En el panel izquierdo, bajo el nodo de árbol **Descripción general del servidor**, se muestran todos los servidores (SLOT-01 a SLOT-04) en la lista de servidores. Si un servidor no está presente en la ranura, la imagen correspondiente en el gráfico aparecerá atenuada. Cuando un servidor de altura completa está presente en la ranura 1 y la ranura 3, la ranura 3 mostrará el nombre de ranura como **Extensión de 1**.

2 Pase el cursor sobre el nombre o el número de ranura de un servidor. Aparece información sobre herramientas con el nombre de modelo del servidor y la etiqueta de servicio (si está disponible).

Visualización del resumen del chasis

Para ver la información del resumen del chasis, en el panel izquierdo, haga clic en **Descripción general del chasis** > **Propiedades** > **Resumen**.

Aparecerá la página **Resumen del chasis**. Para obtener más información sobre esta página, consulte *Online Help* (Ayuda en línea).

Visualización de información y estado de la controladora del chasis

Para ver la información y el estado de la controladora del chasis, en la interfaz web de la CMC, haga clic en **Descripción general del chasis** > **Controladora del chasis**.

Aparecerá la página **Condición de la controladora del chasis**. Para obtener más información, consulte la *Ayuda en línea*.

Visualización de información y estado de condición de todos los servidores

Para ver el estado de condición de todos los servidores, realice alguno de los siguientes pasos:

- Haga clic en **Descripción general del chasis**. La página **Condición del chasis** mostrará una descripción gráfica de todos los servidores instalados en el chasis. Dicha condición se indica mediante la superposición del subgráfico del servidor. Para obtener más información acerca de la función del chasis, consulte la *Ayuda en línea*.
- Haga clic en **Descripción general del chasis** > **Descripción general del servidor**. La página **Estado de los servidores** ofrece una descripción general de los servidores en el chasis. Para obtener más información, consulte la *Ayuda en línea*.

Visualización de información y estado de condición de un servidor individual

Para ver el estado de condición de servidores individuales, realice alguno de los siguientes pasos:

1 Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.

La página **Condición del chasis** mostrará una descripción gráfica de todos los servidores instalados en el chasis. Dicha condición se indica mediante la superposición del subgráfico del servidor. Pase el cursor sobre el subgráfico de un servidor individual. La sugerencia de texto o la explicación en pantalla correspondiente brinda información adicional sobre ese servidor. Haga clic en el subgráfico del servidor para ver la información del módulo de E/S a la derecha. Para obtener más información, consulte la *Ayuda en línea*.

2 Vaya a **Descripción general del chasis** y **expanda la Descripción general del servidor** en el panel izquierdo. Aparecerán todos los servidores (1–4) en la lista expandida. Haga clic en el servidor (ranura) que desea ver.

La página **Estado del servidor** (separada de la página **Estado de los servidores**) proporciona la condición del servidor en el chasis y un punto de inicio para la interfaz web del iDRAC, que es el firmware utilizado para administrar el servidor. Para obtener más información, consulte la *Ayuda en línea*.

NOTA: Para utilizar la interfaz web de iDRAC debe tener un nombre de usuario y una contraseña de iDRAC. Para obtener más información acerca de iDRAC y el uso de la interfaz web del iDRAC, consulte la *Integrated Dell Remote Access Controller User's Guide* (Guía del usuario de Dell Integrated Dell Remote Access Controller.

Visualización de la información y el estado del módulo de E/S

Para ver el estado de condición de los módulos de E/S, en la interfaz web de la CMC, realice alguno de los siguientes pasos:

1 Haga clic en **Descripción general del chasis**.

Aparecerá la página **Estado del chasis**. Los gráficos en el panel izquierdo muestran la vista trasera, frontal y lateral del chasis y contienen el estado del módulo de E/S. El estado del módulo de E/S se indica mediante la superposición del subgráfico del LCD. Mueva el cursor por el subgráfico del módulo de E/S individual. La sugerencia de texto proporciona información adicional acerca del módulo de E/S. Haga clic en el subgráfico para ver la información correspondiente en el panel derecho.

2 Vaya a **Descripción general del chasis** > **Descripción general del módulo de E/S**.

La página **Estado del módulo de E/S** proporciona una descripción general de los módulos de E/S asociados con el chasis. Para obtener más información, consulte la *Ayuda en línea*.

NOTA: Después de actualizar o efectuar un ciclo de encendido del módulo de E/S o agregador de E/S, asegúrese de que el sistema operativo de estos componentes también se inicie correctamente. De lo contrario, el estado del módulo de E/S se muestra como "Desconectado".

Visualización de información y estado de condición de los ventiladores

La CMC controla la velocidad del ventilador del chasis aumentando o disminuyendo dicha velocidad en base a los sucesos del sistema. Es posible ejecutar el ventilador en tres modos: Bajo, Medio y Alto. Para obtener más información acerca de la configuración de los ventiladores, consulte la *Ayuda en línea*.

Para configurar las propiedades de los ventiladores mediante los comandos RACADM, escriba el siguiente comando en la interfaz de CLI.

```
racadm fanoffset [-s <off|low|medium|high>]
```

Para obtener más información acerca de los comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/cmcmanuals**.

NOTA: La CMC supervisa los sensores de temperatura en el chasis y ajusta automáticamente la velocidad del ventilador según sea necesario. Sin embargo, es posible realizar una sustitución para mantener una velocidad mínima del ventilador mediante el comando fanoffset de RACADM. Cuando se modifique mediante este comando, la CMC siempre ejecutará el ventilador en la velocidad seleccionada, aunque el chasis no requiera que los ventiladores se ejecuten a esa velocidad.

La CMC genera una alerta y aumenta la velocidad de los ventiladores cuando se producen los siguientes sucesos:

- Se excede el umbral de temperatura ambiente de la CMC.
- Un ventilador deja de funcionar.
- Se desmonta un ventilador del chasis.

NOTA: Durante las actualizaciones de firmware de la CMC o del iDRAC en un servidor, algunos o todos los ventiladores del chasis funcionan al 100%. Esto es normal.

Para ver el estado de condición de los ventiladores, en la interfaz web de la CMC, realice alguno de los siguientes pasos:

1 Vaya a **Descripción general del chasis**.

Aparecerá la página **Estado del chasis**. La sección inferior de los gráficos del chasis ofrece la vista izquierda del chasis y contiene información del estado de los ventiladores. Dicho estado se indica mediante la superposición del subgráfico del ventilador. Mueva el cursor por el subgráfico del ventilador. La sugerencia de texto ofrece información adicional acerca de un ventilador. Haga clic en el subgráfico del ventilador para ver la información del ventilador en el panel derecho.

2 Vaya a **Descripción general del chasis** > **Ventiladores**.

La página **Estado de los ventiladores** proporciona el estado, las mediciones de velocidad en revoluciones por minuto (RPM) y los valores de umbral de los ventiladores en el chasis. Puede haber uno o varios ventiladores.

NOTA: En caso de una falla de comunicación entre la CMC y el ventilador, la CMC no puede obtener ni mostrar el estado de condición de la unidad del ventilador.

NOTA: Si no hay ventiladores presentes en las ranuras o si un ventilador gira a una velocidad baja, aparece el siguiente mensaje:

```
Fan <number> is less than the lower critical threshold.
```

Para obtener más información, consulte la *Ayuda en línea*.

Configuración de ventiladores

Desplazamiento del ventilador: es una función que ofrece un mayor enfriamiento para el almacenamiento y las regiones de PCIe del chasis. Esta función permite aumentar la distribución de flujo de aire en los HDD, las controladoras PERC compartidas y las ranuras de tarjetas PCIe. Por ejemplo, la opción Desplazamiento del ventilador se recomienda para los usuarios con tarjetas PCIe de energía alta o personalizadas que necesitan más enfriamiento de lo normal. Esta función incluye las opciones Apagado, Bajo, Medio y Alto. Esta configuración corresponde a un desplazamiento de velocidad de ventilador (aumento) del 20%, 50% y 100% de la velocidad máxima respectivamente. También hay un valor mínimo de velocidad PARA cada opción, de 35% para Bajo, 65% para Medio y 100% para Alto.

Por ejemplo, si se utiliza el valor Medio de la función Desplazamiento del ventilador, se aumenta la velocidad de los ventiladores de 1 a 6 en un 50% de su velocidad máxima. Este aumento supera la velocidad ya establecida por el sistema para enfriamiento según la configuración del hardware instalado.

Con cualquiera de las opciones de Desplazamiento del ventilador activadas, aumentará el consumo de alimentación. El sistema será más ruidoso con el desplazamiento Bajo, bastante más ruidoso con el desplazamiento Medio y significativamente ruidoso con el desplazamiento Alto. Cuando la opción Desplazamiento del ventilador no está activada, las velocidades del ventilador se reducen a las velocidades predeterminadas necesarias para enfriar el sistema de la configuración del hardware instalado.

Para establecer la función de desplazamiento, vaya a **Descripción general del chasis** > **Ventiladores** > **Configuración**. En la página **Configuración avanzada del ventilador**, en la tabla **Configuración del ventilador**, del menú desplegable **Valor** que corresponde al **Desplazamiento del ventilador**, seleccione la opción correspondiente.

Para obtener más información sobre la función Desplazamiento del ventilador, consulte la *ayuda en línea*.

Para configurar estas funciones mediante los comandos RACADM, utilice el siguiente comando:

```
racadm fanoffset [-s <off|low|medium|high>]
```

Para obtener más información sobre los comandos RACADM relacionados con la función de desplazamiento del ventilador, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en dell.com/support/Manuals.

Modo de enfriamiento mejorado (ECM) es una función de la CMC que permite aumentar la capacidad de enfriamiento de los servidores instalados en el chasis PowerEdge VRTX. Por ejemplo, puede usar la función ECM en entornos con temperatura ambiente alta o cuando se usan servidores que tienen instalados CPU con energía alta (≥120W). La capacidad de enfriamiento aumentada se logra cuando se les permite a los cuatro módulos de ventilación del chasis operar a una velocidad más alta. Debido a ello, cuando se activa el ECM puede aumentar el consumo de energía del sistema y el nivel de ruido.

Si está activado, el ECM solo aumentará la capacidad de enfriamiento en las ranuras del servidor del chasis. También es importante destacar que el ECM no está diseñado para proporcionarles mayor enfriamiento a los servidores en todo momento. Aunque el ECM esté activado, las velocidades de ventilación más altas solo se registran cuando se necesita más enfriamiento. Algunos ejemplos de esta situación incluyen niveles altos de uso o presión del servidor y temperaturas ambiente elevadas.

De manera predeterminada, el ECM está apagado. Cuando el ECM está activado, la ventilación puede entregar aproximadamente un 20% más de flujo de aire por blade.

Para establecer el modo ECM, vaya a **Descripción general del chasis** > **Ventiladores** > **Configuración**. En la página **Configuración avanzada del ventilador**, en la tabla **Configuración de la turbina**, del menú desplegable **Valor** que corresponde al **Modo de enfriamiento mejorado**, seleccione la opción correspondiente.

Para obtener más información acerca de la función ECM, consulte la *ayuda en línea*.

Visualización de las propiedades del panel frontal

Para ver las propiedades del panel frontal:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Panel frontal**.
2 En la página **Propiedades**, puede ver lo siguiente:
   - **Propiedades del botón de encendido.**
   - **Propiedades de LCD**
   - **Propiedades de KVM**
   - **Propiedades de las unidades de DVD**

Visualización de información y estado de condición del KVM

Para ver el estado de condición de los KVM asociados con el chasis, realice alguno de los siguientes pasos:

1 Haga clic en **Descripción general del chasis**.
   Aparecerá la página **Estado del chasis**. El panel izquierdo muestra la vista frontal del chasis y contiene el estado de un KVM. Dicho estado se indica mediante la superposición del subgráfico del KVM. Mueva el puntero sobre el subgráfico de un KVM para que aparezca la sugerencia de texto o pantalla correspondiente. La sugerencia de texto proporciona información adicional acerca del KVM. Haga clic en el subgráfico del KVM para ver la información correspondiente en el panel derecho.
2 De manera alternativa, haga clic en **Descripción general del chasis** > **Panel anterior**.
   En la página **Estado**, en la sección **Propiedades de KVM**, se pueden ver el estado y las propiedades de un KVM asociado con el chasis. Para obtener más información, consulte la *Ayuda en línea*.

Visualización de información y condición de la pantalla LCD

Para ver el estado de la condición de un LCD:

1 En el panel izquierdo, haga clic en **Descripción general del chasis**.
   Aparecerá la página **Estado del chasis**. El panel izquierdo muestra la vista frontal del chasis. El estado de LCD se indica mediante la superposición del subgráfico del LCD.
2 Mueva el cursor sobre el subgráfico de LCD. La sugerencia de texto o la explicación en pantalla correspondiente brinda información adicional sobre el LCD.
3 Haga clic en el subgráfico de LCD para ver la información de LCD en el panel derecho. Para obtener más información, consulte la *Ayuda en línea*.

De manera alternativa, vaya a **Descripción general del chasis** > **Panel frontal** > **Propiedades** > **Estado**. En la página **Estado**, en **Propiedades de LCD**, puede ver el estado del LCD disponible en el chasis. Para obtener más información, consulte la *Ayuda en línea*.

Visualización de información y estado de condición de los sensores de temperatura

Para ver el estado de condición de los sensores de temperatura:

En el panel izquierdo, haga clic en **Descripción general del chasis** > **Sensores de temperatura**.

La página **Estado de los sensores de temperatura** muestra el estado y la lectura de las sondas de temperatura de todo el chasis (chasis y servidores). Para obtener más información, consulte la *Ayuda en línea*.

NOTA: El valor de las sondas de temperatura no se puede editar. Cualquier cambio fuera del umbral genera una alerta que varía la velocidad del ventilador. Por ejemplo, si la sonda de temperatura ambiente de la CMC excede el umbral, la velocidad de los ventiladores en el chasis aumenta.

Visualización de la capacidad de almacenamiento y el estado de los componentes de almacenamiento

Para ver la capacidad y el estado con tolerancia a errores de los componentes de almacenamiento, realice una de las siguientes acciones:

1 Vaya a **Descripción general del chasis**.

Aparecerá la página **Estado del chasis**. Los detalles de la capacidad de almacenamiento y la información del modo con tolerancia a errores (activo/pasivo) y del estado con tolerancia a errores (activado) aparecen en el panel de la derecha. Esta información sobre la tolerancia a errores aparece solo si la función de la tolerancia a errores está activada para los componentes de almacenamiento.

La sección inferior de los gráficos del chasis proporciona la vista izquierda del chasis. Mueva el cursor por sobre el subgráfico del componente de almacenamiento. La sugerencia de texto ofrece información adicional acerca de un ventilador. Haga clic en el subgráfico del componente de almacenamiento para ver la información relacionada en el panel derecho.

2 De manera alternativa, en el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Propiedades** > **Estado**.

Aparece la página **Descripción general del almacenamiento** con la siguiente información:

- Ver el resumen gráfico de las unidades de discos físicos instaladas en el chasis y su estado.
- Ver el resumen de todos los componentes de almacenamiento con enlaces a sus respectivas páginas.
- Ver la capacidad utilizada y la capacidad total del almacenamiento.
- Ver información de la controladora.

NOTA: En el caso de una controladora con tolerancia a errores, el formato del nombre es: *<número de PERC> compartida (integrada (<número>)*. Por ejemplo, la controladora activa es PERC8 compartida (integrada 1) y la controladora homóloga es PERC8 compartida (integrada 2).

- Ver los sucesos de almacenamiento registrados recientemente.

NOTA: Para obtener más información, consulte la *Ayuda en línea*.

6

Configuración del CMC

Chassis Management Controller permite configurar propiedades, usuario y alertas para realizar tareas de administración remota.

Antes de comenzar a configurar la CMC, es necesario definir primero los valores de configuración de red de la CMC para que esta pueda administrarse de manera remota. Esta configuración inicial asigna los parámetros de red TCP/IP que permiten obtener acceso a la CMC. Para obtener más información, consulte Configuración del acceso inicial a la CMC.

Es posible configurar el CMC por medio de la interfaz web o RACADM.

NOTA: Cuando se configura la CMC por primera vez, se debe iniciar sesión como usuario raíz para ejecutar los comandos RACADM en un sistema remoto. Es posible crear otro usuario con privilegios para configurar la CMC.

Después de configurar el CMC y determinar la configuración básica, puede realizar lo siguiente:

- Si fuera necesario, modifique la configuración de la red.
- Configure las interfaces para obtener acceso al CMC.
- Configure la pantalla LCD.
- Si fuera necesario, configure los grupos de chasis.
- Configure los servidores, el módulo de E/S o el panel anterior.
- Configure los parámetros de VLAN.
- Obtenga los certificados necesarios.
- Agregue y configure los usuarios con privilegios del CMC.
- Configure y active las alertas por correo electrónico y las capturas SNMP.
- Si fuera necesario, establezca la política de límite de alimentación.

NOTA: Los siguientes caracteres no se pueden usar en la cadena de propiedad de las dos interfaces del CMC (interfaz gráfica de usuario y CLI):

- &#
- < y > juntos
- ; (punto y coma)

Temas:

Visualización y modificación de la configuración de red LAN del CMC

Los valores de LAN, como la cadena de comunidad y la dirección IP del servidor SMTP, afectan tanto a la CMC como a la configuración externa del chasis.

Si existen dos CMC (activo y en espera) en el chasis y se conectan a la red, el CMC en espera asume automáticamente la configuración de red del CMC activo en caso de falla.

Cuando IPv6 se activa en el momento del inicio, se envían tres solicitudes de enrutador cada cuatro segundos. Si los switches de red externos ejecutan el Protocolo de árbol de expansión (SPT), es posible que los puertos de los switches externos queden bloqueados durante un plazo mayor a doce segundos en los que se envían las solicitudes de enrutador IPv6. En estos casos, puede haber un período en el que la conectividad de IPv6 sea limitada, hasta que los anuncios de enrutadores sean enviados por el enrutador IPv6 sin ser requeridos.

NOTA: Cambiar la configuración de red de la CMC puede desconectar la conexión de red actual.

NOTA: Es necesario contar con privilegios de Administrador de configuración del chasis para definir la configuración de red de la CMC.

Visualización y modificación de la configuración de red LAN del CMC mediante la interfaz web del CMC

Para ver y modificar la configuración de red LAN de la CMC mediante la interfaz web de la CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, haga clic en **Red**. La página **Configuración de la red** muestra la configuración actual de la red.
2. Modifique la configuración general de IPv4 o IPv6, según sea necesario. Para obtener más información, consulte la *Ayuda en línea*.
3. Haga clic en **Aplicar cambios** para aplicar la configuración en cada sección.

Visualización y modificación de la configuración de red LAN del CMC mediante RACADM

Para ver la configuración de IPv4, utilice los objetos del grupo **cfgCurrentLanNetworking** con los siguientes subcomandos `getniccfg` y `getconfig`.

Para ver la configuración de IPv6, utilice los objetos del grupo **cfgIpv6LanNetworking** con el subcomando `getconfig`.

Para ver la información de direccionamiento de IPv4 e IPv6 para el chasis, use el subcomando `getsysinfo`.

Para obtener más información acerca de los objetos y subcomandos, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Activación de la interfaz de red del CMC

Para activar o desactivar la interfaz de red de la CMC para IPv4 e IPv6, escriba:

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicEnable 0
```

NOTA: El NIC de la CMC está activado de forma predeterminada.

Para activar o desactivar el direccionamiento IPv4 de la CMC, escriba:

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
1
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
0
```

NOTA: El direccionamiento IPv4 del CMC está activado de forma predeterminada.

Para activar o desactivar el direccionamiento IPv6 de la CMC, escriba:

```
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
1
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
0
```

NOTA: Tenga en cuenta lo siguiente:

- Existe un retraso de 30 segundos entre el cambio de la configuración de red y su aplicación real.
- El direccionamiento IPv6 de la CMC está desactivado de forma predeterminada.

De forma predeterminada, para IPv4, la CMC solicita y obtiene automáticamente una dirección IP para la CMC del servidor de Protocolo de configuración dinámica de host (DHCP). Es posible desactivar la función DHCP y especificar la dirección IP, la puerta de enlace y la máscara de subred de la CMC estática.

En una red IPv4, para desactivar el DHCP y especificar dirección IP, puerta de enlace y máscara de subred estáticas para la CMC, escriba:

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgNicIpAddress <static IP address>
racadm config -g cfgLanNetworking -o cfgNicGateway <static gateway>
racadm config -g cfgLanNetworking -o cfgNicNetmask <static subnet mask>
```

De forma predeterminada, para IPv6, el CMC solicita y obtiene automáticamente una dirección IP de la CMC a partir del mecanismo de configuración automática de IPv6.

En una red IPv6, para desactivar la función de configuración automática y especificar dirección IPv6, puerta de enlace y longitud de prefijo estáticas para la CMC, escriba:

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6AutoConfig 0
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Address <IPv6 address>
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6PrefixLength 64
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Gateway <IPv6 address>
```

Activación o desactivación de DHCP para la dirección de interfaz de red del CMC

Cuando se activa, la función DHCP para la dirección de NIC de la CMC solicita y obtiene automáticamente una dirección IP del servidor de protocolo de configuración dinámica de host (DHCP). Esta función está activada de manera predeterminada.

Se puede desactivar la función DHCP para la dirección de NIC y especificar una dirección IP estática, una máscara de subred y una puerta de enlace. Para obtener más información, consulte Configuración del acceso inicial a la CMC.

Activación o desactivación de DHCP para las direcciones IP de DNS

De forma predeterminada, la función DHCP para la dirección de DNS de la CMC está desactivada. Cuando está activada, esta función obtiene las direcciones primarias y secundarias del servidor DNS desde el servidor DHCP. Mientras se usa esta función, no es necesario configurar las direcciones IP estáticas del servidor DNS.

Para desactivar la función DHCP para la dirección de DNS y especificar direcciones estáticas de los servidores DNS preferido y alternativo, escriba:

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

Para activar la función DHCP para la dirección de DNS para IPv6 y especificar direcciones estáticas de los servidores DNS preferido y alternativo, escriba:

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6DNSServersFromDHCP6 0
```

Establecimiento de direcciones IP estáticas de DNS

NOTA: La configuración de direcciones IP estáticas de DNS solo es válida cuando la función de DHCP para la dirección de DNS está desactivada.

En IPv4, para definir las direcciones IP de los servidores DNS primario preferido y secundario, escriba:

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <IP-address>
racadm config -g cfgLanNetworking -o cfgDNSServer2 <IPv4-address>
```

En IPv6, para definir las direcciones IP de los servidores DNS preferido y secundario, escriba:

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6DNSServer1 <IPv6-address>
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6DNSServer2 <IPv6-address>
```

Configuración de los valores de DNS de IPv4 e IPv6

- **Registro de la CMC**: para registrar el CMC en el servidor DNS, escriba:

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

  NOTA: Algunos servidores DNS registran solamente los nombres de 31 caracteres o menos. Asegúrese de que el nombre designado no supere el límite requerido de DNS.

  NOTA: Los siguientes valores solo son válidos si ha registrado el CMC en el servidor DNS al establecer cfgDNSRegisterRac como 1.

- **Nombre de la CMC**: de manera predeterminada, el nombre de la CMC del servidor DNS es cmc-<*service tag*>. Para cambiar el nombre de la CMC en el servidor DNS, escriba:

  ```
  racadm config -g cfgLanNetworking -o cfgDNSRacName <name>
  ```

  donde <*name*> es una cadena de hasta 63 caracteres alfanuméricos y guiones. Por ejemplo: cmc-1, d-345.

  NOTA: Si no se especifica un nombre de dominio DNS, el número máximo de caracteres es 63. Si se especifica un nombre de dominio, el número de caracteres en el nombre de la CMC más el número de caracteres en el nombre del dominio DNS debe ser menor o igual a 63 caracteres.

- **Nombre de dominio DNS**: el nombre predeterminado del dominio DNS es un solo caracter en blanco. Para establecer un nombre de dominio DNS, escriba:

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSDomainName <name>
  ```

  donde <*name*> es una cadena de hasta 254 caracteres alfanuméricos y guiones. Por ejemplo: p45, a-tz-1, r-id-001.

Configuración de la negociación automática, el modo dúplex y la velocidad de la red para IPv4 e IPv6

Cuando se activa, la función de negociación automática determina si el CMC debe establecer automáticamente el modo dúplex y la velocidad de la red mediante la comunicación con el enrutador o el conmutador más cercano. De manera predeterminada, la función de supervisión está activada.

Es posible desactivar la negociación automática y especificar el modo dúplex y la velocidad de la red si se escribe:

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <duplex mode>
```

donde:

duplex mode es 0 (dúplex medio) o 1 (dúplex completo, valor predeterminado)

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <speed>
```

donde:

speed es 10 o 100 (valor predeterminado).

Configuración de la unidad de transmisión máxima para IPv4 e IPv6

La propiedad de unidad de transmisión máxima (MTU) le permite establecer un límite para el paquete más grande que se puede transferir mediante la interfaz. Para definir la MTU, escriba:

```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

donde <*mtu*> es un valor entre 576 y 1500 (inclusive, el valor predeterminado es 1500).

NOTA: IPv6 requiere una MTU mínima de 1280. Si IPv6 está activado y `cfgNetTuningMtu` se ha establecido en un valor inferior, la CMC utiliza una MTU de 1280.

Configuración de las opciones de red y de seguridad de inicio de sesión del CMC

Las funciones de bloqueo de direcciones IP y de bloqueo de usuarios en la CMC le permiten evitar problemas de seguridad provocados por intentos de ataques de contraseñas. Esta función le permite bloquear un rango de direcciones IP y de usuarios que pueden acceder a la CMC. De manera predeterminada, la función de bloqueo de direcciones IP está activada en la CMC. Puede configurar los atributos del rango de IP mediante la interfaz web de la CMC o RACADM. Para usar las funciones de bloqueo de direcciones IP y de bloqueo de usuarios, active las opciones con la interfaz web de la CMC o con RACADM. Configure las opciones de la política de bloqueo de inicio de sesión para establecer la cantidad de intentos de inicio de sesión fallidos para un usuario o una dirección IP específicos. Superado este límite, el usuario bloqueado podrá iniciar sesión solo después de vencido el tiempo de penalidad.

NOTA: El bloqueo por direcciones IP solo puede aplicarse para direcciones IPv4.

Configuración de los atributos de rango de IP con la interfaz web del CMC

NOTA: Para realizar la siguiente tarea, debe tener privilegios de Administrador de configuración del chasis.

Para configurar los atributos de rango de IP mediante la interfaz web del CMC:

1 En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Red** > **Red**. Aparecerá la página **Configuración de red**.

2 En la sección Configuración de IPv4, haga clic en **Opciones avanzadas**.

Aparecerá la página **Seguridad de inicio de sesión**.

De manera alternativa, para acceder a la página Seguridad de inicio de sesión, en el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en**Seguridad** > **Inicio de sesión**.

3 Para activar la función de verificación de rango de IP, en la sección **Rango de IP**, seleccione la opción **Rango de IP activado**.

Se activarán los campos **Dirección de rango de IP** y **Máscara de rango de IP**.

4 En los campos **Dirección de rango de IP** y **Máscara de rango de IP**, escriba el rango de direcciones IP y de máscaras de rangos de IP para los que desea bloquear el acceso al CMC.

Para obtener más información, consulte la *Ayuda en línea*.

5 Haga clic en **Aplicar** para guardar la configuración.

Configuración de los atributos de rango de IP con RACADM

Puede configurar los siguientes atributos de rango de IP para el CMC con RACADM:

- Función de verificación de rango de IP
- Rango de direcciones IP para las que desea bloquear el acceso al CMC
- Máscara del rango de IP para el que desea bloquear el acceso al CMC

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP que se especifica. Solo se autoriza un inicio de sesión de una dirección IP entrante si los dos valores siguientes son idénticos:

- **cfgRacTuneIpRangeMask** en cantidad de bits y con la dirección IP entrante
- **cfgRacTuneIpRangeMask** en cantidad de bits y con **cfgRacTuneIpRangeAddr**

- Para activar la función de verificación de rango IP, use la siguiente propiedad en el grupo `cfgRacTuning`:

  ```
  cfgRacTuneIpRangeEnable <0/1>
  ```

- Para especificar el rango de direcciones IP para las que desea bloquear el acceso a la CMC, use la siguiente propiedad en el grupo `cfgRacTuning`:

  ```
  cfgRacTuneIpRangeAddr
  ```

- Para especificar la máscara del rango de IP para el que desea bloquear el acceso a la CMC, use la siguiente propiedad en el grupo `cfgRacTuning`:

  ```
  cfgRacTuneIpRangeMask
  ```

Configuración de las propiedades de la etiqueta LAN virtual para CMC

La función de LAN virtual permite que varias VLAN coexistan en el mismo cable de red físico y segreguen el tráfico de red por motivos de seguridad o de administración de carga. Cuando se activa la función de VLAN, se asigna una etiqueta VLAN a cada paquete de red.

Configuración de las propiedades de la etiqueta LAN virtual para CMC mediante RACADM

1 Active las capacidades de LAN virtual (VLAN) de la red de administración del chasis externo:

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

2 Especifique la identificación de VLAN para la red de administración del chasis externo:

```
racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
```

Los valores válidos para *VLAN id* son 1 a 4000 y 4021 a 4094. El valor predeterminado es 1.

Por ejemplo:

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

3 A continuación, especifique la prioridad de VLAN para la red de administración del chasis externo:

```
racadm config -g cfgLanNetworking -o
cfgNicVLanPriority <VLAN priority>
```

Los valores válidos para *VLAN priority* son de 0 a 7. El valor predeterminado es 0.

Por ejemplo:

```
racadm config -g cfgLanNetworking -o
cfgNicVLanPriority 7
```

También puede especificar la identificación y la prioridad de VLAN con un solo comando:

```
racadm setniccfg -v <VLAN id> <VLAN priority>
```

Por ejemplo:

```
racadm setniccfg -v 1 7
```

4 Para eliminar la VLAN del CMC, desactive las capacidades de VLAN de la red de administración del chasis externo:

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

También puede eliminar la VLAN del CMC con el siguiente comando:

```
racadm setniccfg -v
```

Configuración de las propiedades de la etiqueta LAN virtual para CMC mediante la interfaz web

Para configurar la LAN virtual (VLAN) para el CMC mediante la interfaz web del CMC:

1 Desplácese a cualquiera de las siguientes páginas:

- En el panel izquierdo, haga clic en **Descripción general del chasis** y luego en **Red** > **VLAN**.
- En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del servidor** y, a continuación, en **Red** > **VLAN**.

Aparecerá la página **Configuración de la etiqueta VLAN**. Las etiquetas VLAN son propiedades del chasis. Permanecen en el chasis aunque se elimine un componente.

2 En la sección **CMC**, active la red VLAN para la CMC, establezca la prioridad y asigne la ID. Para obtener más información acerca de los campos, consulte la *Ayuda en línea*.

3 Haga clic en **Aplicar**. Se guardará la configuración de la etiqueta VLAN.

También puede obtener acceso a esta página a través de **Descripción general del chasis** > **Servidores** > **Configuración** > **VLAN**.

Estándar federal de procesamiento de información

Las agencias y contratistas del gobierno federal de los Estados Unidos utilizan Federal Information Processing Standards (FIPS), un estándar de seguridad de computadoras, que se relaciona con todas las aplicaciones que tienen interfaces de comunicación. El 140-2 consta de cuatro niveles: nivel 1, nivel 2, nivel 3 y nivel 4. El FIPS de la serie 140-2 estipula que todas las interfaces de comunicación deben tener las siguientes propiedades de seguridad:

- Autentificación
- Confidencialidad
- Integridad del mensaje
- No rechazo
- Disponibilidad
- control de acceso

Si alguna de las propiedades depende de algoritmos criptográficos, los FIPS deben autorizar estos algoritmos.

El modo FIPS está desactivado de forma predeterminada. Cuando se activa FIPS, el tamaño de clave mínimo para OpenSSL FIPS es de 2048 bits RSA de SSH-2.

NOTA: Cuando se activa el modo FIPS en el chasis, no se admite la actualización del firmware de la unidad de suministro de alimentación.

Para obtener más información, consulte *CMC Online Help* (Ayuda en línea para la CMC).

Las siguientes funciones/aplicaciones admiten FIPS.

- GUI web
- RACADM
- WSMan
- SSH v2
- SMTP
- Kerberos
- Cliente de NTP
- NFS

NOTA: SNMP no es compatible con FIPS. En el modo FIPS, todas las funciones de SNMP son operativas, excepto la autentificación del algoritmo de Resumen del mensaje versión 5 (MD5).

Activación del modo FIPS mediante la interfaz web de la CMC

Para activar FIPS:

1 En el panel izquierdo, haga clic en **Descripción general del chasis**.
Aparecerá la página **Estado del chasis**.
2 En la barra de menús, haga clic en **Impresora**.
Aparecerá la página **Configuración de red**.
3 En la sección **Federal Information Processing Standards (FIPS)** en el menú desplegable **modo FIPS**, seleccione **Activado**.
Aparece un mensaje que indica que la activación FIPS restablece la CMC a los valores predeterminados.
4 Haga clic en **OK** (Aceptar) para continuar.

Configuración del modo de FIPS mediante RACADM

Para activar el modo FIPS, ejecute el siguiente comando:

```
racadm config –g cfgRacTuning –o cfgRacTuneFipsModeEnable 1
```

.

Desactivación del modo FIPS

Para desactivar el modo FIPS, reinicie el CMC con la configuración predeterminada de fábrica.

Configuración de servicios

Es posible configurar y activar los servicios siguientes en la CMC:

- Consola serie de la CMC: permita el acceso a la CMC mediante la consola serie.
- Servidor web: permita el acceso a la interfaz web de la CMC. La desactivación del servidor web también desactiva el RACADM remoto.
- SSH: permita el acceso a la CMC mediante la funcionalidad RACADM de firmware.
- Telnet: permita el acceso a la CMC mediante la funcionalidad RACADM de firmware.
- RACADM: permita el acceso al CMC mediante la funcionalidad RACADM.
- SNMP: active la CMC para enviar capturas SNMP para los sucesos.
- Syslog remoto: active el CMC para registrar sucesos en un servidor remoto. Para usar esta función, debe tener una licencia Enterprise.

La CMC incluye un servidor web configurado para usar el protocolo de seguridad estándar en la industria SSL para aceptar y transferir datos cifrados desde y hacia los clientes a través de la Internet. El servidor web incluye un certificado digital SSL autofirmado de Dell (ID del servidor) y tiene la responsabilidad de aceptar y responder solicitudes HTTP seguras de los clientes. La interfaz web y la herramienta CLI remota de RACADM requieren este servicio para comunicarse con la CMC.

Si se restablece el servidor web, espere al menos un minuto para que los servicios estén nuevamente disponibles. El restablecimiento del servidor web puede producirse como consecuencia de alguno de los siguientes sucesos:

- La configuración de red o las propiedades de seguridad de la red se modificaron a través de la interfaz de usuario web del CMC o RACADM.
- La configuración del puerto de Web Server se modificó a través de la interfaz de usuario web o RACADM.
- Se restablece la CMC.
- Se carga un nuevo certificado del servidor SSL.

NOTA: Para modificar los ajustes de los servicios, deberá tener privilegios de Administrador de configuración del chasis.

El syslog remoto es un destino de registro adicional para la CMC. Después de configurar el syslog remoto, cada nueva anotación de registro generada por CMC se reenviará a los respectivos destinos.

NOTA: Puesto que el transporte de red para las anotaciones de registro reenviadas es UDP, no se garantiza que las anotaciones de registro se entreguen ni que el CMC reciba comentarios para indicar si las anotaciones se recibieron correctamente.

Configuración de los servicios mediante la interfaz web del CMC

Para configurar los servicios del CMC mediante la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, haga clic en **Red** > **Servocios**. Se muestra la página **Administración de servicios**.

2 Configure los servicios siguientes según sea necesario:

- Serie CMC
- Servidor web
- SSH
- Telnet
- RACADM remoto
- SNMP
- Syslog remoto

Para obtener información acerca de los campos, consulte la *Ayuda en línea*.

3 Haga clic en **Aplicar** y luego actualice todos los límites de tiempo de espera predeterminados y máximos.

Configuración de servicios mediante RACADM

Para activar y configurar los distintos servicios, utilice los siguientes objetos RACADM:

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Para obtener más información acerca de estos objetos, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en dell.com/support/manuals.

Si el firmware en el servidor no admite una función, la configuración de una propiedad relacionada con esa función muestra un error. Por ejemplo, si se utiliza RACADM para activar el syslog remoto en un iDRAC no compatible, aparecerá un mensaje de error.

De forma similar, al mostrar las propiedades del iDRAC mediante el comando `getconfig` de RACADM, los valores de las propiedades aparecerán como N/A para una función no admitida en el servidor.

Por ejemplo:

```
$ racadm getconfig -g cfgSessionManagement -m server-1
# cfgSsnMgtWebServerMaxSessions=N/A
# cfgSsnMgtWebServerActiveSessions=N/A
# cfgSsnMgtWebServerTimeout=N/A
# cfgSsnMgtSSHMaxSessions=N/A
# cfgSsnMgtSSHActiveSessions=N/A
# cfgSsnMgtSSHTimeout=N/A
# cfgSsnMgtTelnetMaxSessions=N/A
# cfgSsnMgtTelnetActiveSessions=N/A
# cfgSsnMgtTelnetTimeout=N/A
```

Configuración de la tarjeta de almacenamiento extendido del CMC

Es posible activar o reparar los medios flash extraíbles opcionales para utilizarlos como un almacenamiento extendido no volátil. Algunas funciones de la CMC dependen de un almacenamiento extendido no volátil para funcionar.

Para activar o reparar los medios flash extraíbles mediante la interfaz web de la CMC:

1 En el panel izquierdo, vaya a **Descripción general del chasis** y, a continuación, haga clic en **Controladora del chasis** > **Medios flash**.

2 En la página **Medios flash extraíbles**, en el menú desplegable, seleccione una de las siguientes opciones según corresponda:

- **Reparar medios del controlador activo**
- **Detener el uso de los medios flash para almacenar datos del chasis**

Para obtener más información sobre estas opciones, consulte *Online Help* (Ayuda en línea).

3 Haga clic en **Aplicar** para aplicar la opción seleccionada.

Si dos CMC están presentes en el chasis, los dos CMC (activo y en estado de espera) deben contener medios flash. De lo contrario, la funcionalidad de almacenamiento extendido debe estar degradado a menos que los CMC activo y en estado de espera contengan medios flash.

Configuración de un grupo de chasis

La CMC le permite controlar varios chasis desde un solo chasis principal. Cuando se activa un grupo de chasis, la CMC del chasis principal genera un gráfico sobre el estado del chasis principal y de los demás chasis del grupo. Para usar esta función, debe tener una licencia Enterprise.

Las funciones del grupo de chasis son las siguientes:

- Muestra imágenes con la parte delantera y posterior de cada chasis; un conjunto para el chasis principal y un conjunto para cada miembro.
- Los problemas en la condición del chasis principal y de los miembros de un grupo se marcan en rojo o amarillo y con una X o un ! en el componente que muestra los síntomas. Los detalles se muestran debajo de la imagen del chasis al hacer clic en la imagen o los **Detalles** del chasis.
- Los vínculos de inicio rápido están disponibles para abrir las páginas web del servidor o del chasis miembro.
- Hay un servidor y un inventario de entradas/salidas disponibles para un grupo.
- Existe una opción seleccionable para sincronizar las propiedades del miembro nuevo con las propiedades del principal cuando el miembro nuevo se agrega al grupo.

Un grupo de chasis puede tener un máximo de ochos chasis miembros. Asimismo, un chasis principal o miembro sólo puede participar de un grupo. No se puede unir un chasis, ya sea principal o miembro, a otro grupo si ya forma parte de otro grupo. Es posible eliminar el chasis de un grupo y agregarlo más adelante a un grupo diferente.

Para configurar el grupo de chasis mediante la interfaz web de la CMC:

1 Inicie sesión en el chasis principal con los privilegios de administrador de chasis.

2 Haga clic en **Configuración** > **Administración de grupos**.

3 En la página **Grupo de chasis**, en **Función**, seleccione **Chasis principal**. Aparecerá un campo para agregar el nombre de grupo.

4 Introduzca el nombre de grupo en el campo **Nombre del grupo** y haga clic en **Aplicar**.

NOTA: Los nombres de dominio siguen las mismas reglas.

Cuando se crea el grupo de chasis, la interfaz gráfica de usuario pasa automáticamente a la página **Grupo de chasis**. El panel izquierdo indica el grupo por nombre de grupo y el chasis principal y el chasis miembro no completado aparecen en el panel izquierdo.

Adición de miembros a un grupo de chasis

Después de configurar el grupo de chasis, para añadir miembros al grupo:

1 Inicie sesión en el chasis principal con los privilegios de administrador de chasis.
2 Seleccione el chasis principal en el árbol.
3 Haga clic en **Configuración** > **Administración de grupos**.
4 En **Administración de grupos**, introduzca el nombre de DNS o la dirección IP del miembro en el campo **Nombre del host/Dirección IP**.
5 En el campo **Nombre de usuario** introduzca un nombre de usuario con privilegios de administrador para el chasis miembro.
6 Introduzca la contraseña correspondiente en el campo **Contraseña**.
7 Si lo desea, seleccione **Sincronizar el miembro nuevo con las propiedades del principal** para insertar las propiedades del chasis principal al miembro.
8 Haga clic en **Aplicar**.
9 Para agregar un máximo de ocho miembros, complete las tareas del paso 4 al 8. Los nombres del chasis de los nuevos miembros aparecen en el cuadro de diálogo **Miembros**.

NOTA: Las credenciales introducidas para un miembro se deben transmitir en forma segura al chasis miembro, para establecer una relación de confianza entre el miembro y el chasis principal. Las credenciales no se conservan en ninguno de los chasis y nunca se vuelven a intercambiar después de que se establece la relación de confianza inicial.

Eliminación de un miembro del chasis principal

Es posible eliminar un miembro del grupo desde el chasis principal. Para eliminar un miembro:

1 Inicie sesión en el chasis principal con los privilegios de administrador de chasis.
2 En el panel izquierdo, seleccione el chasis principal.
3 Haga clic en **Configuración** > **Administración de grupos**.
4 En la lista **Eliminar miembros**, seleccione el nombre de los miembros que desea eliminar y, a continuación, haga clic en **Aplicar**.

El chasis principal establecerá una conexión con el miembro o los miembros, si se selecciona más de uno, que se hayan eliminado del grupo. Se elimina el nombre del miembro. Si no se produce un contacto entre el miembro y el chasis principal debido a un problema en la red, es posible que el chasis miembro no reciba el mensaje. En ese caso, desactive el miembro del chasis miembro para poder quitarlo totalmente.

Forma de desmontar un grupo de chasis

Para extraer totalmente un grupo del chasis principal:

1 Inicie sesión en el chasis principal con privilegios de administrador.
2 Seleccione el chasis principal en el panel izquierdo.
3 Haga clic en **Configuración** > **Administración de grupos**.
4 En la página **Grupo de chasis**, en **Función**, seleccione **Ninguno** y, a continuación, haga clic en **Aplicar**.

El chasis principal luego comunica a todos los miembros que han sido eliminados del grupo. El chasis principal se puede asignar como chasis líder o chasis miembro de un grupo nuevo.

Si un problema de red evita el contacto entre el chasis líder y el chasis miembro, este último puede no recibir el mensaje. En este caso, desactive el miembro del chasis miembro para completar el proceso de eliminación.

Desactivación de un miembro del chasis miembro

En ocasiones, no se puede quitar un miembro de un grupo mediante el chasis principal. Esto se produce si se pierde la conectividad de red con el miembro. Para eliminar un miembro de un grupo en el chasis miembro:

1 Inicie sesión en el chasis miembro con privilegios de administrador.
2 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Configuración** > **Administración de grupos**.
3 Seleccione **Ninguno** y, a continuación, haga clic en **Aplicar**.

Acceso a la página web de un chasis miembro o servidor

Es posible acceder a la página web del chasis miembro, la consola remota del servidor o la página web del servidor iDRAC desde la página del grupo de chasis principal. Si el dispositivo miembro tiene las mismas credenciales de inicio de sesión que el chasis principal, puede usar las mismas credenciales para acceder al dispositivo miembro.

NOTA: No se admiten el inicio de sesión único ni el inicio de sesión mediante tarjeta inteligente en la administración de varios chasis. Para acceder a los miembros por medio del inicio de sesión único desde el chasis principal se requiere un nombre de usuario o una contraseña común entre el chasis principal y los miembros. El uso de un nombre de usuario o una contraseña común solamente funciona con usuarios de Active Directory, locales y de LDAP.

Para desplazarse a los dispositivos miembro:

1 Inicie sesión en el chasis principal.
2 Seleccione **Grupo: nombre** en el árbol.
3 Si el destino necesario es una CMC miembro, seleccione **Iniciar CMC** para el chasis necesario.

Si el destino necesario es un servidor en un chasis, realice lo siguiente:

a Seleccione la imagen del chasis de destino.
b En la imagen del chasis que aparece en la sección **Condición**, seleccione el servidor.
c En el cuadro con la etiqueta **Vínculos de acceso rápido**, seleccione el dispositivo de destino. Aparecerá una nueva ventana con la pantalla de inicio de sesión o la página de destino.

NOTA: En MCM, no se muestran todos los vínculos de acceso rápido asociados con los servidores.

Propagación de las propiedades del chasis principal al chasis miembro

Puede aplicar las propiedades del chasis principal al chasis miembro de un grupo. Para sincronizar un miembro con las propiedades del chasis principal:

1 Inicie sesión en el chasis principal con privilegios de administrador.
2 Seleccione el chasis principal en el árbol.
3 Haga clic en **Configuración** > **Administración de grupos**.
4 En la sección **Propagación de las propiedades del chasis** seleccione un tipo de propagación:
   - Propagación ante cambio: seleccione esta opción para propagar automáticamente la configuración de las propiedades del chasis seleccionadas. Los cambios de propiedades se propagan a todos los miembros del grupo actual cada vez que se cambien las propiedades del chasis principal.
   - Propagación manual: seleccione esta opción para propagar manualmente las propiedades del chasis principal del grupo con sus miembros. La configuración de las propiedades del chasis principal se propaga a los miembros del grupo solo cuando el administrador del chasis principal hace clic en **Propagar**.
5 En la sección **Propiedades de propagación**, seleccione las categorías de las propiedades de configuración del chasis principal a propagar a los chasis miembro.

Seleccione solo las categorías que desee que cuenten con una configuración idéntica en todos los miembros del grupo de chasis. Por ejemplo, seleccione la categoría **Propiedades de registro y alerta** para permitir que todos los chasis del grupo compartan la configuración de registro y alertas del chasis principal.

6 Haga clic en **Guardar**.

Si está seleccionada la opción **Propagación ante cambio**, el chasis miembro toma las propiedades del chasis principal. Si está seleccionada la opción **Propagación manual**, haga clic en **Propagar** cada vez que desee propagar la configuración elegida al chasis miembro. Para obtener más información acerca de la propagación de propiedades del chasis principal a los chasis miembro, consulte la *Ayuda en línea*.

Inventario del servidor para el grupo de MCM

Un grupo es un chasis principal que contiene entre 0 y 8 miembros. En la página **Condición del grupo de chasis** se muestran todos los chasis miembro y se puede guardar el informe de inventario del servidor en un archivo, con la capacidad de descarga estándar del explorador. El informe contiene datos para:

- Todos los servidores presentes actualmente en todos los chasis del grupo (incluido el principal).
- Las ranuras vacías y las ranuras de extensión (incluidos los módulos del servidor de altura total y de doble ancho).

Forma de guardar el informe de inventario del servidor

Para guardar el informe de inventario del servidor mediante la interfaz web de la CMC:

1 En el panel izquierdo, seleccione el **Grupo**.

2 En la página **Condición del grupo de chasis**, haga clic en **Guardar informe de inventario**. Se mostrará el cuadro de diálogo **Descarga de archivo**, donde se le solicitará que abra o guarde el archivo.

3 Haga clic en **Guardar** y especifique la ruta de acceso y el nombre de archivo para el informe de inventario del módulo del servidor.

NOTA: El grupo de chasis principal y el grupo de chasis de miembro, así como el módulo del servidor del chasis asociado, deben estar encendidos para poder obtener el informe de inventario del módulo más preciso.

Datos exportados

El informe de inventario del servidor contiene los datos más recientes que cada miembro del grupo de chasis ha devuelto durante el sondeo normal del líder del grupo de chasis (una vez cada 30 segundos).

Para obtener el informe de inventario del servidor más preciso posible:

- El chasis principal y todos los chasis miembro del grupo se deben encontrar en **Estado de alimentación del chasis encendido**.
- Todos los servidores en el chasis asociado deben estar encendidos.

Es posible que el informe de inventario no incluya los datos de inventario para el chasis asociado y los servidores si un subconjunto del chasis miembro del grupo se encuentra:

- En estado **de alimentación del chasis apagado**
- Apagado

NOTA: Si se inserta un servidor mientras el chasis está apagado, el número de modelo no se muestra en ningún lado en la interfaz web hasta que el chasis se vuelve a encender.

En la siguiente tabla se enumeran los campos de datos y los requisitos específicos para los campos que se deben incluir en el informe sobre cada servidor:

Tabla 17. Descripciones de los campos de inventario del módulo del servidor

Campo de datos	Ejemplo
Nombre del chasis	Chasis principal del centro de datos
Dirección IP del chasis	192.168.0.1
Ubicación de ranura	1
Nombre de ranura	RANURA-01
Nombre del host	Web Server corporativo **NOTA: Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.**
Sistema operativo	Windows Server 2008 **NOTA: Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.**
Modelo	PowerEdgeM610
Etiqueta de servicio	1PB8VF1
Memoria total del sistema	4.0 GB **NOTA: Requiere VRTX CMC 1.0 (o posterior) en el miembro; de lo contrario, se mostrará en blanco.**
N.º de CPU	2 **NOTA: Requiere VRTX CMC 1.0 (o posterior) en el miembro; de lo contrario, se mostrará en blanco.**
Información de CPU	CPU Intel (R) Xeon (R) E5502 a 1.87 GHzn **NOTA: Requiere VRTX CMC 1.0 (o posterior) en el miembro; de lo contrario, se mostrará en blanco.**

Formato de datos

El informe de inventario se genera en un formato de archivo .CSV, para poder importarlo a varias herramientas, como, por ejemplo, Microsoft Excel. El archivo .CSV del informe de inventario se puede importar en la plantilla al seleccionar **Datos** > **Desde texto** en MS Excel. Una vez que el informe de inventario se haya importado en MS Excel, si aparece un mensaje para solicitar información adicional, seleccione Delimitado por comas para importar el archivo en MS Excel.

Inventario del grupo de chasis y versión de firmware

La página **Versión de firmware del grupo de chasis** muestra el inventario de grupos y las versiones de firmware de los servidores y los componentes del servidor en el chasis. Esta página también le permite organizar la información de inventario y filtrar la vista de las versiones de firmware. La vista mostrada puede basarse en los servidores o en cualquiera de los siguientes componentes del servidor del chasis:

- BIOS
- iDRAC
- CPLD
- USC
- Diagnóstico
- Controladores de SO

- RAID
- NIC

NOTA: La información de inventario mostrada en cuanto a grupo de chasis, chasis miembro, servidores y componentes de servidores se actualiza cada vez que se agrega o se elimina un chasis del grupo.

Visualización del inventario del grupo de chasis

Para ver el grupo de chasis mediante la interfaz web de la CMC, en el panel izquierdo, seleccione **Grupo**. Haga clic en **Propiedades** > **Versión de firmware**. La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.

Visualización del inventario del chasis seleccionado con la interfaz web

Para ver el inventario del chasis seleccionado con la interfaz web del CMC:

1 En el árbol del sistema, seleccione el **Grupo**. haga clic en **Propiedades** > **Versión de firmware**.
La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.

2 En la sección **Seleccionar un chasis**, seleccione el chasis miembro del que desea ver el inventario.
La sección **Filtro de visualización de firmware** muestra el inventario de servidor del chasis seleccionado y las versiones de firmware de todos los componentes del servidor.

Visualización de las versiones de firmware de los componentes de servidor seleccionados con la interfaz web

Para ver las versiones de firmware de los componentes de servidores seleccionados mediante la interfaz web del CMC:

1 En el panel izquierdo, seleccione el **Grupo**. Haga clic en **Propiedades** > **Versión de firmware**.
La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.

2 En la sección **Seleccionar un chasis**, seleccione el chasis miembro del que desea ver el inventario.

3 En la sección **Filtro de visualización de firmware**, seleccione **Componentes**.

4 En la lista **Componentes**, seleccione el componente requerido (BIOS, iDRAC, CPLD, USC, Diagnóstico, unidad de SO, dispositivos RAID [hasta 2] y dispositivos NIC [hasta 6]) para los que desea ver la versión de firmware.
Aparecerán las versiones de firmware del componente seleccionado de todos los servidores en el chasis miembro seleccionado.

Perfiles de configuración del chasis

La función Perfiles de configuración del chasis le permite configurar el chasis con los perfiles de configuración del chasis almacenados en el recurso compartido de red o la estación de administración local y también restaurar la configuración del chasis.

Para acceder a la página **Perfiles de configuración del chasis** en la interfaz web de la CMC, en el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Configuración** > **Perfiles**. Aparece la página **Perfiles de configuración del chasis**.

Puede realizar las siguientes tareas mediante la función Perfiles de configuración del chasis:

- Configurar un chasis mediante perfiles de configuración del chasis en la estación de administración local para la configuración inicial.
- Guardar los valores de configuración del chasis actuales en un archivo XML en el recurso compartido de red o en la estación de administración local.
- Restaurar la configuración del chasis.

- Importar perfiles del chasis (archivos XML) al recurso compartido de red desde una estación de administración local.
- Exportar perfiles del chasis (archivos XML) desde el recurso compartido de red a una estación de administración local.
- Aplicar, editar, eliminar o exportar una copia de los perfiles almacenados en el recurso compartido de red.

Cómo guardar la configuración del chasis

Puede guardar la configuración del chasis actual en un archivo XML en un recurso compartido de red o en la estación de administración local. Las configuraciones incluyen todas las propiedades del chasis que se pueden modificar mediante la interfaz web de la CMC y los comandos de RACADM. También puede utilizar el archivo XML que se guarda para restaurar la configuración en el mismo chasis o para configurar otro chasis.

NOTA: Los valores de configuración del servidor y del iDRAC no se guardan ni se restauran con la configuración del chasis.

Para guardar la configuración actual del chasis, realice las siguientes tareas:

1 Diríjase a la página **Perfiles de configuración del chasis**. En la sección **Guardar y hacer copia de seguridad** > **Guardar configuración actual**, introduzca un nombre para el perfil en el campo **Nombre del perfil**.

NOTA: Al guardar la configuración del chasis actual, se admite el conjunto de caracteres extendidos ASCII estándar. No obstante, no se admiten los siguientes caracteres especiales:

“, ., *, >, <, \, /, :, y |

2 Seleccione uno de los siguientes tipos de perfil desde la opción **Tipo de perfil**:

- **Reemplazar**: incluye atributos de toda la configuración de la CMC excepto los atributos de solo escritura, como por ejemplo, contraseñas de usuario y etiquetas de servicio. Este tipo de perfil se utiliza como un archivo de configuración de copia de seguridad para restaurar la configuración del chasis completo, que incluye información de identidad, como las direcciones IP.
- **Clon**: incluye todos los atributos de perfil del tipo **Reemplazar**. Los atributos de identidad, como por ejemplo, dirección MAC y la dirección IP se indican por motivos de seguridad. Este tipo de perfil se usa para clonar un chasis nuevo.

3 Seleccione una de las siguientes ubicaciones del menú desplegable **Ubicación del perfil** para almacenar el perfil:

- **Local**: para guardar el perfil en la estación de administración local.
- **Recurso compartido de red**: para guardar el perfil en la ubicación del recurso compartido.

4 Haga clic en **Guardar** para guardar el perfil en la ubicación seleccionada.

Una vez finalizada la acción, aparece el mensaje `Operation Successful`

NOTA: Para ver los valores guardados en el archivo XML, en la sección Perfiles almacenados, seleccione el perfil guardado y haga clic en Ver en la columna Ver perfiles.

Restauración del perfil de configuración del chasis

Puede restaurar la configuración de un chasis al importar el archivo de copia de seguridad (.xml o .bak) en la estación de administración local o el recurso compartido de red en el que se ha guardado la configuración del chasis. Las configuraciones incluyen todas las propiedades disponibles a través de la interfaz web de la CMC, los comandos de RACADM y los valores de configuración.

Para restaurar la configuración del chasis, realice las siguientes tareas:

1 Diríjase a la página **Perfiles de configuración del chasis**. En la sección **Restaurar configuración** > **Restaurar configuración del chasis**, haga clic en **Examinar** y seleccione el archivo de copia de seguridad para importar la configuración del chasis guardada.

2 Haga clic en **Restaurar configuración** para cargar un archivo de copia de seguridad cifrado (.bak) o un archivo de perfil almacenado .xml en la CMC.

La interfaz web de la CMC regresa a la página de inicio de sesión después de una operación de restauración satisfactoria.

NOTA: Si los archivos de copia de seguridad (.bak) de las versiones anteriores de la CMC se cargan en la versión más reciente de la CMC donde FIPS está activado, vuelva a configurar las 16 contraseñas de usuario local de la CMC. Sin embargo, la contraseña del primer usuario se restablece a "calvin".

NOTA: Cuando un perfil de configuración del chasis se importa desde una CMC (que no admite la función FIPS) a una CMC donde FIPS está activado, el FIPS permanece activado en la CMC.

NOTA: Si cambia el modo FIPS en el perfil de configuración del chasis, se activa la opción `DefaultCredentialMitigation`.

Visualización de perfiles de configuración del chasis almacenados

Para ver los perfiles de configuración del chasis almacenados en el recurso compartido de red, vaya a la página **Perfiles de configuración del chasis**. En la sección **Perfiles de configuración del chasis** > **Perfiles almacenados**, seleccione el perfil y haga clic en **Ver** en la columna **Ver perfil**. Aparece la página **Ver configuración**. Para obtener más información sobre la configuración visualizada, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Aplicación de perfiles de configuración del chasis

Puede aplicar la configuración del chasis al chasis si los perfiles de configuración del chasis están disponibles como perfiles almacenados en el recurso compartido de red. Para iniciar una operación de configuración del chasis, puede aplicar un perfil almacenado a un chasis.

Para aplicar un perfil a un chasis, realice las siguientes tareas:

1. Diríjase a la página **Perfiles de configuración del chasis**. En la sección **Perfiles almacenados**, seleccione el perfil almacenado que desea aplicar.
2. Haga clic en **Aplicar perfil**.

   Aparece un mensaje de aviso de que al aplicar un nuevo perfil se sobrescribe la configuración actual y también se reinician los chasis seleccionados. Se le pide que confirme si desea continuar con la operación.
3. Haga clic en **Aceptar** para aplicar el perfil al chasis.

Cómo exportar perfiles de configuración del chasis

Puede exportar perfiles de configuración del chasis guardados en el recurso compartido de red a una ruta de acceso especificada en una estación de administración.

Para exportar un perfil almacenado, realice las siguientes tareas:

1. Diríjase a la página **Perfiles de configuración del chasis**. En la sección **Perfiles de configuración del chasis** > **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Exportar copia del perfil**.

   Aparecerá el cuadro de diálogo **Descarga de archivo**, donde se le solicitará que abra o guarde el archivo.
2. Haga clic en **Guardar** o **Abrir** para exportar el perfil en la ubicación requerida.

Edición de perfiles de configuración del chasis

Puede editar el nombre del perfil de configuración del chasis de un chasis.

Para editar un nombre de perfil de configuración del chasis, realice las siguientes tareas:

1. Diríjase a la página **Perfiles de configuración del chasis**. En la sección **Perfiles de configuración del chasis** > **Perfiles almacenados**, seleccione el perfil necesario y haga clic en **Editar perfil**.

   Aparecerá la ventana **Editar perfil**.
2. Introduzca un nombre de perfil deseado en el campo **Nombre de perfil** y haga clic en **Editar perfil**.

   Aparecerá el mensaje `Operation Successful`.
3. Haga clic en **OK** (Aceptar).

Eliminación de perfiles de configuración del chasis

Puede eliminar un perfil de configuración del chasis almacenado en el recurso compartido de red.

Para eliminar un perfil de configuración del chasis, realice las siguientes tareas:

1 Diríjase a la página **Perfiles de configuración del chasis**. En la sección **Perfiles de configuración del chasis** > **Perfiles almacenados**, seleccione el perfil necesario y haga clic en **Eliminar perfil**.

Aparecerá un mensaje de advertencia donde se indica que al eliminar un perfil se eliminará permanentemente el perfil seleccionado.

2 Haga clic en **Aceptar** para eliminar el perfil seleccionado.

Configuración de varios CMC mediante RACADM

Por medio de RACADM, es posible configurar uno o varios CMC con propiedades idénticas.

Cuando se realiza una consulta en una tarjeta de CMC específica con su ID de grupo e ID de objeto, RACADM crea el archivo de configuración `racadm.cfg` en función de la información recuperada. Al exportar el archivo a una o varias CMC, es posible configurar las controladoras con propiedades idénticas en un tiempo mínimo.

NOTA: Algunos archivos de configuración contienen información exclusiva del CMC (como la dirección IP estática) que se debe modificar antes de exportar el archivo a otros CMC.

1 Use RACADM para hacer una consulta en el CMC de destino que contiene la configuración deseada.

NOTA: El archivo de configuración generado es myfile.cfg. Puede cambiar el nombre del archivo. El archivo .cfg no contiene contraseñas de usuario. Cuando el archivo .cfg se carga en la nueva CMC, se deben volver a agregar todas las contraseñas.

2 En el símbolo del sistema, escriba:

```
racadm getconfig -f myfile.cfg
```

NOTA: El redireccionamiento de la configuración de la CMC hacia un archivo por medio de `getconfig -f` solo se admite con la interfaz de RACADM remoto.

3 Modifique el archivo de configuración con un editor de texto simple (opcional). Cualquier caracter de formato especial en el archivo de configuración puede dañar la base de datos de RACADM.

4 Use el archivo de configuración recientemente creado para modificar una CMC de destino. En el símbolo del sistema, escriba:

```
racadm config -f myfile.cfg
```

5 Restablezca la CMC de destino que se había configurado. En el símbolo del sistema, escriba:

```
racadm reset
```

El subcomando `getconfig -f myfile.cfg` solicita la configuración de la CMC para la CMC activa y genera el archivo **myfile.cfg**. Si es necesario, puede cambiar el nombre del archivo o guardarlo en una ubicación diferente.

Es posible utilizar el comando `getconfig` para realizar las siguientes acciones:

- Mostrar todas las propiedades de configuración en un grupo (especificado por el nombre del grupo y el índice);
- Mostrar todas las propiedades de configuración de usuario por nombre de usuario.

El subcomando `config` carga la información en otras CMC. El Administrador del servidor utiliza el comando `config` para sincronizar la base de datos de usuario y contraseña.

Creación de un archivo de configuración del CMC

El archivo de configuración de la CMC, **<filename>.cfg** se utiliza con el comando `racadm config -f <filename>.cfg` para crear un archivo de texto simple. El comando le permite generar un archivo de configuración (de forma parecida a un archivo **.ini**) y configurar la CMC a partir de este archivo.

Se puede utilizar cualquier nombre de archivo y el archivo no requiere una extensión **.cfg** (aunque en este apartado se haga referencia al archivo con esa denominación).

NOTA: Para obtener más información sobre este subcomando `getconfig`, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

RACADM analiza el archivo **.cfg** cuando se carga por primera vez en la CMC para verificar que contenga nombres de grupo y objeto válidos y que se cumplan las reglas de sintaxis básicas. Los errores se indican con el número de línea que ha detectado el error, y un mensaje explica el problema. Se analiza todo el archivo para verificar su integridad y se muestran todos los errores. Si se encuentra un error en el archivo **.cfg**, los comandos de escritura no se transmiten a la CMC. El usuario debe corregir todos los errores antes de poder realizar cualquier configuración.

Para verificar si existen errores antes de crear el archivo de configuración, utilice la opción `-c` con el subcomando. `config` Con la opción `-c`, `config` solo verifica la sintaxis y no escribe en la CMC.

Siga estas pautas para crear un archivo **.cfg**:

- Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.
  El analizador lee todos los índices de la CMC para ese grupo. Todos los objetos dentro de ese grupo son modificaciones cuando se configura la CMC. Si un objeto modificado representa un índice nuevo, el índice se crea en la CMC durante la configuración.
- El usuario no puede especificar un índice deseado en un archivo **.cfg**.
  Los índices se pueden crear y eliminar. Con el tiempo, el grupo se puede fragmentar con índices utilizados y no utilizados. Si existe un índice, se lo modifica. Si no existe, se utiliza el primer índice disponible.

  Este método ofrece flexibilidad al agregar anotaciones indexadas en las que no es necesario establecer coincidencias exactas del índice entre todas las CMC que se administran. Se agregan nuevos usuarios al primer índice disponible. Un archivo **.cfg** que se analiza y se ejecuta correctamente en una CMC podría no ejecutarse correctamente en otra si todos los índices están llenos y se debe agregar un nuevo usuario.
- Use el subcomando `racresetcfg` para configurar ambas CMC con propiedades idénticas.
  Utilice el subcomando `racresetcfg` para restablecer la CMC a sus valores predeterminados originales y, a continuación, ejecute el comando. `racadm config -f <filename>.cfg` Asegúrese de que el archivo **.cfg** incluya todos los objetos, usuarios, índices y demás parámetros requeridos. Para una lista completa de objetos y grupos, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

  PRECAUCIÓN: Utilice el subcomando `racresetcfg` para restablecer la configuración de la base de datos y de la Interfaz de red de la CMC a sus valores originales predeterminados, y elimine todos los usuarios y las configuraciones de usuario. Aunque el usuario raíz está disponible, los demás valores de configuración de usuarios también se restablecen a los valores predeterminados.
- Si escribe `racadm getconfig -f <filename> .cfg`, el comando crea un archivo **.cfg** para la configuración actual de la CMC. Este archivo de configuración se puede usar como un ejemplo y como punto de inicio para su archivo **.cfg** único.

Reglas de análisis

- Las líneas que comienzan con un carácter numeral (#) se tratan como comentarios.

Una línea de comentario debe comenzar en la columna uno. Un carácter '#' en cualquier otra columna se trata como un carácter '#'.

Algunos parámetros de modem podrían incluir caracteres '#' en sus cadenas. No se requiere un carácter de escape. Es posible que quiera generar un archivo **.cfg** de un comando `racadm getconfig -f <filename> .cfg` y luego, ejecutar un comando `racadm config -f <filename> .cfg` para una CMC diferente, sin agregar caracteres de escape.

Por ejemplo:

```
#
# This is a comment
[cfgUserAdmin]
cfgUserAdminPageModemInitString= <Modem init # not
a comment>
```

- Todas las anotaciones de grupos deben estar entre corchetes de apertura y de cierre ([y]).

  El carácter de apertura "[" que indica un nombre de grupo debe estar en la columna uno. Este nombre de grupo debe especificarse antes de cualquiera de los objetos de ese grupo. Los objetos que no incluyen un nombre de grupo asociado generarán errores. Los datos de configuración se organizan en grupos, como se define en el capítulo de propiedad de base de datos de la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM Chassis Management Controller para PowerEdge VRTX). En el siguiente ejemplo se muestra un nombre de grupo, un objeto y el valor de la propiedad del objeto.

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object name}
{object value}
```

- Todos los parámetros están especificados como pares "objeto=valor" sin espacios en blanco entre el objeto, el símbolo "=" y el valor. Los espacios en blanco que se incluyan después de un valor se omiten. Un espacio en blanco dentro de una cadena de valores se mantendrá sin modificación. El carácter que se encuentre a la derecha del signo = (por ejemplo, un segundo signo =, #, [,], etc.) se considerará "tal cual". Estos caracteres son caracteres de secuencia de comandos de chat de módem válidos.

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object value}
```

- El analizador del archivo **.cfg** ignora una anotación de objeto de índice.

  El usuario no puede especificar el índice que se debe utilizar. Si el índice ya existe, se utiliza ese o se crea la nueva anotación en el primer índice disponible de dicho grupo.

  El comando `racadm getconfig -f <filename>.cfg` coloca un comentario frente a los objetos de índice, lo que permite ver los comentarios incluidos.

  NOTA: Es posible crear un grupo indexado manualmente mediante el siguiente comando:

  ```
  racadm config -g <groupname>  -o <anchored object> -i <index 1-4> <unique anchor name>
  ```

- La línea de un grupo indexado no se puede eliminar de un archivo **.cfg**. Si se elimina la línea con un editor de texto, RACADM se detendrá al analizar el archivo de configuración y generará una alerta sobre el error.

  El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

```
racadm config -g <groupname>  -o <objectname> -i <index 1-4> ""
```

  NOTA: Una cadena NULA (que se identifica con dos caracteres ") indica al CMC que elimine el índice para el grupo especificado.

  Para ver el contenido de un grupo indexado, utilice el siguiente comando:

```
racadm getconfig -g <groupname> -i <index 1-4>
```

- Para los grupos indexados, el ancla del objeto debe ser el primer objeto después del par [ ]. A continuación, se proporcionan ejemplos de los grupos indexados actuales:

```
[cfgUserAdmin]
cfgUserAdminUserName= <USER_NAME>
```

- Cuando se utiliza RACADM remoto para capturar los grupos de configuración en un archivo, si no se define una propiedad clave dentro del grupo, el grupo de configuración no se guardará como parte del archivo de configuración. Si es necesario clonar estos grupos de configuración en otras CMC, se debe definir la propiedad clave antes de ejecutar el comando `getconfig -f`. De manera alternativa, puede introducir manualmente las propiedades faltantes en el archivo de configuración después de ejecutar el comando `getconfig -f`. Esto se aplica a todos los grupos indexados de RACADM.

Esta es la lista de todos los grupos indexados que exhiben este comportamiento y sus propiedades clave correspondientes:

- cfgUserAdmin — cfgUserAdminUserName
- cfgEmailAlert — cfgEmailAlertAddress
- cfgTraps — cfgTrapsAlertDestIPAddr
- cfgStandardSchema — cfgSSADRoleGroupName
- cfgServerInfo — cfgServerBmcMacAddress

Modificación de la dirección IP del CMC

Cuando modifica la dirección IP de la CMC en el archivo de configuración, extraiga todas las entradas `<variable> = <value>` innecesarias. Solo permanecerá la etiqueta del grupo de la variable real con [y], incluyendo las dos entradas `<variable> = <value>` relacionadas con el cambio de dirección IP.

Por ejemplo:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Este archivo se actualiza de la siguiente forma:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

El comando `racadm config -f <myfile>.cfg` analiza el archivo e identifica los errores por número de línea. Un archivo correcto actualiza las anotaciones correctas. Además, puede usar el mismo comando `getconfig` en el ejemplo anterior para confirmar la actualización.

Utilice este archivo para descargar cambios que abarcan toda la empresa o para configurar nuevos sistemas en la red con el comando `racadm getconfig -f <myfile>.cfg`.

NOTA: *Anchor* es una palabra reservada y no se debe utilizar en el archivo .cfg.

Configuración de varias CMC a través de RACADM mediante los perfiles de configuración de chasis

Con los perfiles de configuración del chasis, puede exportar los perfiles de configuración del chasis como un archivo XML e importarlos a otro chasis.

Utilice el comando RACADM **get** para la operación de exportación y el comando **set** para la operación de importación. Puede exportar perfiles del chasis (archivos XML) desde la CMC al recurso compartido de red o a una estación de administración local e importar los perfiles del chasis (archivos XML) desde el recurso compartido de red o desde una estación de administración local.

NOTA: De manera predeterminada, la exportación se realiza como tipo de clon. Puede utilizar el `--clone` para obtener el perfil del tipo de clon en un archivo XML.

La operación de importación y exportación hacia y desde el recurso compartido de red se puede realizar a través del RACADM local, así como el RACADM remoto. En cambio, la operación de importación y exportación hacia y desde la administración local solo puede realizarse a través de la interfaz del RACADM remoto.

Cómo exportar perfiles de configuración del chasis

Puede exportar perfiles de configuración del chasis al recurso compartido de red mediante el comando **get**.

1 Para exportar los perfiles de configuración del chasis como archivo **clone.xml** al recurso compartido de red CIFS mediante **get**, escriba lo siguiente:

```
racadm get -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
```

2 Para exportar los perfiles de configuración del chasis como archivo **clone.xml** al recurso compartido de red NFS mediante el comando **get**, escriba lo siguiente:

```
racadm get -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
```

Puede exportar perfiles de configuración del chasis al recurso compartido de red a través de una interfaz de RACADM remota.

1 Para exportar los perfiles de configuración del chasis como archivo clone.xml al recurso compartido de red CIFS, escriba lo siguiente:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l //xx.xx.xx.xx/
PATH -u USERNAME -p PASSWORD
```

2 Para exportar los perfiles de configuración del chasis como archivo clone.xml al recurso compartido de red NFS, escriba lo siguiente:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l xx.xx.xx.xx:/
PATH
```

Puede exportar perfiles de configuración del chasis a la estación de administración local a través de una interfaz de RACADM remota.

1 Para exportar los perfiles de configuración del chasis como archivo clone.xml, escriba lo siguiente:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml
```

Cómo importar perfiles de configuración del chasis

Puede importar perfiles de configuración del chasis desde un recurso compartido de red a otro chasis mediante el comando **set**.

1 Para importar los perfiles de configuración del chasis desde el recurso compartido de red CIFS, escriba lo siguiente:

```
racadm set -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
```

2 Para importar los perfiles de configuración del chasis desde el recurso compartido de red NFS, escriba lo siguiente:

```
racadm set -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
```

Puede importar perfiles de configuración del chasis desde el recurso compartido de red a través de una interfaz de RACADM remota.

1 Para importar los perfiles de configuración del chasis desde el recurso compartido de red CIFS, escriba lo siguiente:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC  set -f clone.xml -t xml -l //
xx.xx.xx.xx/PATH -u USERNAME -p PASSWORD
```

2 Para importar los perfiles de configuración del chasis desde el recurso compartido de red NFS, escriba lo siguiente:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml -l xx.xx.xx.xx:/
PATH
```

Puede importar perfiles de configuración del chasis desde la estación de administración local a través de una interfaz de RACADM remota.

1 Para exportar los perfiles de configuración del chasis como archivo clone.xml, escriba lo siguiente:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml
```

Reglas de análisis

Usted puede editar manualmente las propiedades de un archivo XML exportado de los perfiles de configuración del chasis.

Un archivo XML contiene las siguientes propiedades:

- **Configuración del sistema**, que es el nodo principal.
- **componente**, que es el nodo dependiente primario.
- **Atributos**, que contiene el nombre y el valor. Puede editar estos campos. Por ejemplo, puede editar el valor `Asset Tag` como se indica a continuación:

  ```
  <Attribute Name="ChassisInfo.1#AssetTag">xxxxxx</Attribute>
  ```

A continuación se menciona un ejemplo de un archivo XML:

```
<SystemConfiguration Model="PowerEdge M1000e
"ServiceTag="NOBLE13"
TimeStamp="Tue Apr  7 14:17:48 2015" ExportMode="2">
<!--Export type is Replace-->
<!--Exported configuration may contain commented attributes. Attributes may be commented due to
dependency,
destructive nature, preserving server identity or for security reasons.-->
<Component FQDD="CMC.Integrated.1">
<Attribute Name="ChassisInfo.1#AssetTag">00000</Attribute>
<Attribute Name="ChassisLocation.1#DataCenterName"></Attribute>
<Attribute Name="ChassisLocation.1#AisleName"></Attribute>
<Attribute Name="ChassisLocation.1#RackName"></Attribute>
….
</Component>
</SystemConfiguration>
```

Visualización y terminación de sesiones en el CMC

Puede ver el número de usuarios actualmente conectados en el iDRAC7 y terminar las sesiones de usuario.

NOTA: Para terminar una sesión, debe tener privilegios de Administrador de configuración del chasis.

Visualización y terminación de sesiones en el CMC mediante la interfaz web

Para ver o terminar una sesión mediante la interfaz web:

1 En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Red** > **Sesiones**.
La página **Sesiones** muestra la ID de la sesión, el nombre de usuario, la dirección IP y el tipo de sesión. Para obtener más información sobre estas propiedades, consulte la *Ayuda en línea*.

2 Para finalizar la sesión, haga clic en **Terminar** para una sesión.

Visualización y terminación de sesiones en el CMC mediante RACADM

Es necesario disponer de privilegios de administrador para terminar sesiones en el CMC mediante RACADM.

Para ver las sesiones de usuario actual, utilice el comando `getssninfo`.

Para terminar una sesión de usuario, utilice el comando `closessn`.

Para obtener más información acerca de estos comandos, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support/manuals**.

7

Configuración de servidores

Es posible configurar los siguientes valores de un servidor:

- Nombres de las ranuras
- Configuración de red del iDRAC
- Configuración de etiqueta LAN virtual del DRAC
- Primer dispositivo de inicio
- Servidor FlexAddress
- Recurso compartido de archivos remotos
- Configuración del BIOS mediante una copia idéntica del servidor

Temas:

Configuración de nombres de las ranuras

Los nombres de las ranuras se utilizan para identificar servidores individuales. Al elegir los nombres de las ranuras, se aplican las siguientes reglas:

- Los nombres pueden contener un máximo de 24 caracteres ASCII no extendidos (códigos ASCII del 32 al 126). Se permite el uso de caracteres estándar y especiales en los nombres.
- Los nombres de las ranuras deben ser únicos dentro del chasis. Las ranuras no deben tener el mismo nombre.
- Las cadenas no distinguen entre mayúsculas y minúsculas. `Server-1, server-1, and SERVER-1` son nombres equivalentes.
- Los nombres de las ranuras no deben comenzar con las siguientes cadenas:
  - Switch-
  - Fan-
  - PS-
  - DRAC-
  - MC-
  - Chasis
  - Housing-Left
  - Housing-Right
  - Housing-Center
- Las cadenas de `Server-1` a `Server-4` se pueden utilizar, pero solo para la ranura correspondiente. Por ejemplo, `Server-3` es un nombre válido para la ranura 3, pero no para la ranura 4. Sin embargo, `Server-03` es un nombre válido para cualquier ranura.

NOTA: Para cambiar un nombre de ranura, debe tener privilegios de Administrador de configuración del chasis.

El valor de los nombres de las ranuras en la interfaz web reside en la CMC solamente. Si un servidor se retira del chasis, la configuración de los nombres de las ranuras no se conservará en el servidor.

El valor de cada nombre de ranura en la interfaz web del CMC siempre suprime cualquier cambio que se aplique al nombre para mostrar en la interfaz del iDRAC.

Para editar un nombre de ranura mediante la interfaz web del CMC:

1 En el panel izquierdo, vaya a **Descripción general del chasis** > **Descripción general del servidor** > **Configuración** > **Nombres de ranura**.
2 En la página **Nombres de ranura**, edite el nombre de ranura, en el campo **Nombre de ranura**.
3 Para usar el nombre de host del servidor como nombre de ranura, seleccione la opción **Utilizar nombre de host para el nombre de ranura**. Esto suprime los nombres de ranuras estáticos por el nombre de host del servidor (o nombre del sistema), si se encuentra disponible. Se requiere que el agente de OMSA esté instalado en el servidor. Para obtener más información sobre el agente de OMSA, consulte la *Guía del usuario de Dell OpenManage Server Administrator,* disponible en dell.com/support/manuals.
4 Para utilizar el nombre de DNS del iDRAC como nombre de ranura, seleccione la opción **Utilizar nombre de DNS del iDRAC para el nombre de ranura**. Esta opción sustituye los nombres de ranura estáticos por los nombres de DNS del iDRAC correspondientes, si se encuentra disponible. Si los nombres de DNS del iDRAC no están disponibles, se muestran los nombres de las ranuras predeterminados o editados.

NOTA: Para seleccionar la opción Utilizar nombre de DNS del iDRAC para el nombre de ranura, debe tener privilegio de Administrador de configuración del chasis.

5 Para guardar la configuración, haga clic en **Aplicar**.

Para restaurar el nombre de ranura predeterminado (de SLOT-01 a SLOT-04, según la posición de la ranura de un servidor) en un servidor, haga clic en **Restaurar valor predeterminado**.

Establecimiento de la configuración de red del iDRAC

Para usar esta función, debe tener una licencia Enterprise. Puede configurar los valores de la red del iDRAC de un servidor. Puede usar la configuración de QuickDeploy para establecer los valores predeterminados de la red del iDRAC y la contraseña raíz para los servidores que se instalen más adelante. Estos ajustes predeterminados constituyen la configuración de QuickDeploy del iDRAC.

Para obtener más información sobre la iDRAC, consulte la *iDRAC User's Guide* (Guía del usuario del iDRAC) en **dell.com/support/manuals**.

Configuración de los valores de red de QuickDeploy del iDRAC

Use la configuración de QuickDeploy para establecer la configuración de la red de los servidores recién insertados.

Para activar y definir la configuración de QuickDeploy de iDRAC:

1 En el panel izquierdo, haga clic en **Descripción general del servidor** > **Configuración** > **iDRAC**.
2 En la sección **Configuración de QuickDeploy**, especifique la configuración que se muestra en la siguiente tabla. Para obtener más información acerca de los campos, consulte la *Ayuda en línea*.

Tabla 18. Configuración de QuickDeploy

Configuración	Descripción
Acción cuando el servidor está insertado	Seleccione una de las siguientes opciones de la lista: • Sin acción: no se realiza ninguna acción cuando el servidor está insertado. • Únicamente QuickDeploy: seleccione esta opción para aplicar la configuración de red del iDRAC cuando se inserta un servidor nuevo en el chasis. La configuración de implementación automática especificada se usa para configurar el nuevo

Configuración	Descripción
	iDRAC, incluida la contraseña de usuario raíz si se selecciona Cambiar contraseña raíz. • Perfil del servidor solamente: seleccione esta opción para aplicar el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis. • QuickDeploy y perfil del servidor: seleccione esta opción para aplicar primero la configuración de red del iDRAC y, a continuación, el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis. .
Definir contraseña root del iDRAC al insertar servidor	Selecciona esta opción para cambiar la contraseña raíz del iDRAC de modo que coincida con el valor ingresado en el campo **Contraseña raíz del iDRAC**, en donde está insertado un servidor.
Contraseña root del iDRAC	Cuando se seleccionan las opciones **Definir contraseña raíz del iDRAC al insertar servidor** y **QuickDeploy activada**, este valor de contraseña se asigna a la contraseña de usuario raíz del iDRAC de un servidor cuando se inserta el servidor en el chasis. La contraseña puede tener de 1 a 20 caracteres imprimibles (incluidos los espacios).
Confirmar contraseña root del iDRAC	Permite volver a escribir la contraseña que figura en el campo **Contraseña**.
Activar LAN del iDRAC	Activa o desactiva el canal LAN del iDRAC. De forma predeterminada, esta opción está desactivada.
Activar IPv4 del iDRAC	Activa o desactiva IPv4 en el iDRAC. De forma predeterminada, esta opción está seleccionada.
Activar la IPMI en la LAN del iDRAC	Activa o desactiva IPMI en el canal de LAN para cada iDRAC presente en el chasis. De forma predeterminada, esta opción está seleccionada.
Activar DHCP de IPv4 del iDRAC	Activa o desactiva el DHCP para cada iDRAC presente en el chasis. Si se activa esta opción, los campos **IP de QuickDeploy, Máscara de subred de QuickDeploy** y **Puerta de enlace de QuickDeploy** se desactivan y no se pueden modificar debido a que se utilizará DHCP para asignar automáticamente estos valores a cada iDRAC. Para seleccionar esta opción, debe seleccionar la opción **Activar IPv4 del iDRAC**. La dirección IP de QuickDeploy se proporciona con dos opciones: 2 y 4.
Dirección IPv4 inicial del iDRAC (ranura 1)	Especifica la dirección IP estática del iDRAC del servidor en la ranura 1 del gabinete. La dirección IP de cada iDRAC subsiguiente se incrementa en 1 para cada ranura a partir de la dirección IP estática de la ranura 1. En el caso donde la suma de la dirección IP y del número de ranura sea mayor que la máscara de subred, se mostrará un mensaje de error. **NOTA: La máscara de subred y la puerta de enlace no se incrementan como la dirección IP.** Por ejemplo, si la dirección IP inicial es `192.168.0.250` y la máscara de subred es `255.255.0.0`, la dirección IP de QuickDeploy para la ranura 15 es `192.168.0.265`. Si la máscara de subred es `255.255.255.0`, aparece este mensaje de error `QuickDeploy IP address range is not fully within QuickDeploy Subnet` al hacer clic en **Guardar configuración de QuickDeploy** o **Completar automáticamente con la configuración de QuickDeploy**.
Máscara de red IPv4 del iDRAC	Especifica la máscara de subred de QuickDeploy que se asigna a todos los servidores recién insertados.
Puerta de enlace IPv4 del iDRAC	Especifica la puerta de enlace predeterminada de QuickDeploy que se asigna a todos los DRAC presentes en el chasis.

Configuración	Descripción
Activar IPv6 del iDRAC	Activa la dirección IPv6 de cada iDRAC presente en el chasis que es compatible con IPv6.
Activar la configuración automática de IPv6 del iDRAC	Activa el iDRAC para obtener la configuración de IPv6 (dirección y longitud de prefijo) de un servidor DHCPv6 y también activa la configuración automática de dirección sin estado. De forma predeterminada, esta opción está activada.
Puerta de enlace IPv6 del iDRAC	Especifica la puerta de enlace predeterminada IPv6 para asignarla a los iDRAC. El valor predeterminado es "::".
Longitud del prefijo IPv6 del iDRAC	Especifica la longitud del prefijo para asignar a las direcciones IPv6 del iDRAC. El valor predeterminado es 64.
Utilice los valores de DNS de la CMC	Comunica los valores de configuración del servidor DNS de la CMC (IPv4 e IPv6) al iDRAC cuando se inserta un servidor blade en el chasis.

3 Haga clic en **Guardar configuración de QuickDeploy** para guardar la configuración. Si ha realizado cambios en la configuración de red del iDRAC, haga clic en **Aplicar configuración de red del iDRAC** para implementar la configuración en el iDRAC.

La función QuickDeploy solamente se ejecuta cuando está activada y se inserta un servidor en el chasis. Si **Establecer contraseña raíz del iDRAC al insertar servidor** y **QuickDeploy activada** están activadas, mediante la interfaz LCD se pedirá al usuario que permita o impida el cambio de la contraseña. Si existen valores de configuración de la red que difieren de la configuración actual del iDRAC, se le pedirá al usuario que acepte o rechace los cambios.

NOTA: Si existe una diferencia de LAN o IPMI en LAN, se solicita al usuario que acepte el valor de dirección IP de QuickDeploy. Si la diferencia es el valor de DHCP, se le solicita al usuario que acepte el valor de QuickDeploy para DHCP.

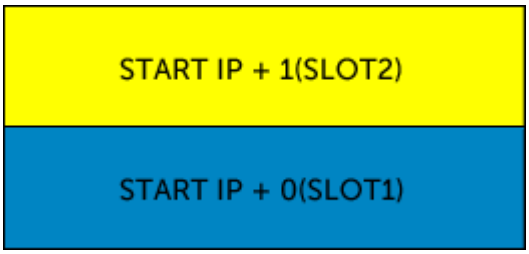
Para copiar la configuración de QuickDeploy a la sección **Configuración de red del iDRAC**, haga clic en **Completar automáticamente con la configuración de QuickDeploy**. Los valores de configuración de red de QuickDeploy se copian en los campos correspondientes de la tabla **Valores de configuración de red del iDRAC**.

NOTA: Los cambios realizados en los campos de QuickDeploy son inmediatos, pero es posible que en el caso de cambios realizados en uno o más valores de configuración de red del servidor iDRAC se necesiten varios minutos para que se propaguen de la CMC al iDRAC. Al hacer clic en Actualizar sin esperar unos minutos, es posible que solo se muestren datos parcialmente correctos para uno o más servidores del iDRAC.

Asignación de dirección IP de QuickDeploy para servidores

La ilustración muestra la asignación de direcciones IP de QuickDeploy a los servidores cuando existen cuatro servidores de altura media en el chasis VRTX:

La ilustración siguiente muestra la asignación de direcciones IP de QuickDeploy a los servidores cuando existen dos blades de altura media en el chasis VRTX:



Modificación de la configuración de red del iDRAC en un servidor individual

Con esta función, es posible configurar los valores de configuración de red del iDRAC para cada servidor instalado. Los valores iniciales que se muestran para cada campo son los valores actuales leídos desde el iDRAC. Para usar esta función, debe tener una licencia Enterprise.

Para modificar la configuración de red del iDRAC:

1 En el panel izquierdo, haga clic en **Descripción general del servidor** y, a continuación, haga clic en **Configuración**. En la página **Implementar el iDRAC**, la sección **Configuración de red del iDRAC** enumera los valores de configuración de red IPv4 e IPv6 del iDRAC de todos los servidores instalados.

2 Modifique la configuración de red del iDRAC según sea necesario para los servidores.

NOTA: Se debe seleccionar la opción Activar LAN para especificar la configuración de IPv4 o IPv6. Para obtener información acerca de los campos, consulte la *Ayuda en línea*.

3 Para implementar la configuración en el iDRAC, haga clic en **Aplicar los valores de configuración de la red del iDRAC**. Los cambios realizados en la **Configuración de QuickDeploy** también se guardarán.

La tabla **Configuración de red del iDRAC** refleja los valores de configuración de red futuros; los valores mostrados para servidores instalados pueden o no ser los mismos valores de configuración de red del iDRAC instalados actualmente. Haga clic en **Actualizar** para actualizar la página **Implementación del iDRAC** con cada valor de configuración de red del iDRAC instalado después de realizar los cambios.

NOTA: Los cambios realizados en los campos de QuickDeploy son inmediatos, pero es posible que en el caso de cambios realizados en uno o más valores de configuración de red del servidor iDRAC se necesiten varios minutos para que se propaguen de la CMC al iDRAC. Al hacer clic en Actualizar sin esperar unos minutos, es posible que solo se muestren datos parcialmente correctos para uno o más servidores del iDRAC.

Modificación de la configuración de red del iDRAC mediante RACADM

Los comandos `config` o `getconfig` de RACADM admiten la opción `-m <module>` para los siguientes grupos de configuración:

- `cfgLanNetworking`
- `cfgIPv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

Para obtener más información sobre los valores y los intervalos predeterminados de las propiedades, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Configuración de los valores de la etiqueta LAN virtual del iDRAC

Las etiquetas LAN virtual (VLAN) se utilizan para permitir que varias VLAN coexistan en el mismo cable de red físico y para segregar el tráfico de red por motivos de seguridad o de administración de carga. Cuando se activa la función de VLAN, se asigna una etiqueta VLAN a cada paquete de red. Las etiquetas VLAN son propiedades del chasis. Permanecen en el chasis aunque se elimine un componente.

NOTA: La ID de VLAN configurada mediante la CMC se aplica a iDRAC solo cuando el iDRAC se encuentra en modo dedicado. Si el iDRAC está en modo LOM compartido, los cambios de ID de VLAN realizados en el iDRAC no se muestran en la interfaz gráfica de usuario de la CMC.

Configuración de los valores de la etiqueta LAN virtual del iDRAC mediante RACADM

- Especifique la identificación y la prioridad de LAN virtual de un servidor específico con el siguiente comando:

  ```
  racadm setniccfg -m server-<n> -v <VLAN id> <VLAN priority>
  ```

  Los valores válidos para <*n*> son de 1 a 4.

  Los valores válidos para <*VLAN*> son de 1 a 4000 y de 4021 a 4094. El valor predeterminado es 1.

  Los valores válidos para <*VLAN priority*> son de 0 a 7. El valor predeterminado es 0.

  Por ejemplo:

  ```
  racadm setniccfg -m server-1 -v 1 7
  ```

  Por ejemplo:

- Para eliminar la VLAN de un servidor, desactive las capacidades de VLAN de la red del servidor especificado:

  ```
  racadm setniccfg -m server-<n> -v
  ```

  Los valores válidos para <*n*> son de 1 a 4.

  Por ejemplo:

  ```
  racadm setniccfg -m server-1 -v
  ```

Configuración de los valores de la etiqueta LAN virtual del iDRAC mediante la interfaz web

Para configurar la LAN virtual (VLAN) del servidor:

1 Desplácese a cualquiera de las siguientes páginas:
   - En el panel izquierdo, haga clic en **Descripción general del chasis** > **Red** > **VLAN**.
   - En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del servidor** y haga clic en **Configuración** > **VLAN**.

2 En la página **Configuración de la etiqueta VLAN**, en la sección **iDRAC**, active VLAN para los servidores, establezca la prioridad e introduzca la ID. Para obtener más información acerca de los campos, consulte la *Ayuda en línea*.

3 Haga clic en **Aplicar** para guardar la configuración.

Configuración del primer dispositivo de inicio

El usuario puede especificar el primer dispositivo de inicio de la CMC para cada servidor. Este puede no ser el primer dispositivo de inicio real para el servidor o incluso puede no representar un dispositivo existente en ese servidor. Representa un dispositivo enviado por la CMC al servidor y que se utilizó como el primer dispositivo de inicio de ese servidor. Es posible establecer este dispositivo como primer dispositivo de inicio predeterminado o dispositivo de inicio para una sola vez a fin de poder iniciar una imagen que realice tareas como ejecutar diagnósticos o reinstalar un sistema operativo.

Puede configurar el primer dispositivo de inicio solo para el siguiente inicio o para todos los reinicios posteriores. También puede configurar el primer dispositivo de inicio para el servidor. El sistema se inicia desde el dispositivo seleccionado en los próximos reinicios y permanece como el primer dispositivo de inicio en el orden de inicio del BIOS, hasta que se cambie nuevamente desde la interfaz web de la CMC (**Descripción general del chasis** > **Descripción general del servidor** > **Configuración** > **Primer dispositivo de inicio**) o desde la secuencia de inicio del BIOS.

NOTA: La configuración del primer dispositivo de inicio en la interfaz web de la CMC suprime la configuración de inicio del BIOS del sistema.

El dispositivo de inicio que especifique debe existir y contener medios iniciables.

Es posible establecer los siguientes dispositivos para el primer inicio.

Tabla 19. Dispositivos de inicio

Dispositivo de inicio	Descripción
PXE	Inicio a partir de un protocolo de entorno de ejecución previa al inicio (PXE) en la tarjeta de interfaz de red.
Unidad de disco duro	Inicio a partir del disco duro del servidor.
CD/DVD local	Inicio a partir de una unidad de CD/DVD en el servidor.
Disco flexible virtual	Inicio a partir de la unidad de disco flexible virtual. La unidad de disco flexible (o una imagen del disco flexible) se encuentra en otro equipo en la red de administración y se conecta a través del visor de consola de la interfaz gráfica de usuario del iDRAC.
CD/DVD virtual	Inicio a partir de una unidad de CD/DVD virtual o de una imagen ISO de CD/DVD. La unidad óptica o el archivo de imagen ISO se encuentra en otro equipo o disco de inicio disponible en la red de administración y se conecta a través del visor de consola de la interfaz gráfica de usuario del iDRAC.
Tarjeta SD local	Inicio a partir de la tarjeta SD (Secure Digital) local, solo para servidores que admiten sistemas iDRAC6 e iDRAC7.
Disco flexible local	Inicio a partir de un disco flexible en la unidad de disco flexible local.
Recurso compartido de archivos remotos	Inicio a partir de una imagen de recurso compartido de archivos remotos (RFS). El archivo de imagen se adjunta mediante el visor de la consola de la interfaz gráfica de usuario del iDRAC.

Configuración del primer dispositivo de inicio para varios servidores mediante la interfaz web del CMC

NOTA: Para configurar el primer dispositivo de inicio para los servidores, es necesario contar con privilegios de administrador Server Administrator o de Administrador de configuración del chasis y privilegios de Inicio de sesión en el iDRAC.

Para configurar el primer dispositivo de inicio para varios servidores:

1 En el panel izquierdo, haga clic en **Descripción general del servidor** > **Configuración** > **Primer dispositivo de inicio**. Se muestra una lista de servidores.
2 En la columna **Primer dispositivo de inicio** del menú desplegable que corresponde al servidor, seleccione el dispositivo de inicio que desea usar para cada servidor.
3 Si desea que el servidor utilice el dispositivo seleccionado cada vez que se inicia, deje en blanco la opción **Boot Once** (Iniciar una vez). Si desea que el servidor utilice el dispositivo seleccionado solo en el siguiente ciclo de inicio, seleccione la opción **Boot Once** (Iniciar una vez) para dicho servidor.
4 Haga clic en **Aplicar** para guardar la configuración.

Configuración del primer dispositivo de inicio para un servidor individual mediante la interfaz web del CMC

NOTA: Para configurar el primer dispositivo de inicio para los servidores, es necesario contar con privilegios de Server Administrator o de Administrador de configuración del chasis y privilegios de Inicio de sesión en el iDRAC.

Para configurar el primer dispositivo de inicio para servidores individuales:

1 En el panel izquierdo, haga clic en **Descripción general del servidor** y haga clic en el servidor para el cual desea configurar el primer dispositivo de inicio.
2 Vaya a **Configuración** > **Primer dispositivo de inicio**. Aparece la pantalla **Primer dispositivo de inicio**.
3 En el menú desplegable **Primer dispositivo de inicio**, seleccione el dispositivo de inicio que desea usar para cada servidor.
4 Si desea que el servidor utilice el dispositivo seleccionado cada vez que se inicia, deje en blanco la opción **Boot Once** (Iniciar una vez). Si desea que el servidor utilice el dispositivo seleccionado solo en el siguiente ciclo de inicio, seleccione la opción **Boot Once** (Iniciar una vez) para dicho servidor
5 Haga clic en **Aplicar** para guardar la configuración.

Configuración del primer dispositivo de inicio mediante RACADM

Para establecer el primer dispositivo de inicio, utilice el objeto `cfgServerFirstBootDevice`.

Para activar el inicio único de un dispositivo, utilice el objeto `cfgServerBootOnce`.

Para obtener más información acerca de estos objetos, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en dell.com/support/manuals.

Configuración de FlexAddress para el servidor

Para obtener información acerca de cómo configurar FlexAddress para servidores, consulte Configuración de FlexAddress para redes Fabric y ranuras a nivel del chasis mediante la interfaz web de la CMC. Para usar esta función, debe tener una licencia Enterprise.

Configuración de recurso compartido de archivos remotos

La función Recurso compartido de archivos de medios virtuales remotos asigna un archivo de una unidad compartida en la red a uno o varios servidores mediante la CMC con el fin de implementar o actualizar un sistema operativo. Cuando se encuentra conectado, es posible

obtener acceso al archivo remoto en forma similar a un archivo al que se puede acceder en un servidor local. Se admiten dos tipos de medio: unidades de disco y unidades de CD/DVD.

Para realizar una operación de recurso compartido de archivos remotos (conectar, desconectar o implementar), debe tener privilegios de **Administrador de configuración del chasis** o de **Administrador del servidor**. Para usar esta función, debe tener una licencia Enterprise.

NOTA: Si está utilizando CIFS que son parte de un dominio de Active Directory, ingrese el nombre del dominio con la dirección IP en la ruta del archivo de imagen.

Para configurar el recurso compartido de archivos remoto:

1 En el panel izquierdo, haga clic en **Descripción general del servidor** > **Configuración** > **Recurso compartido de archivos remoto**.

2 En la página **Implementar recurso compartido de archivos remotos**, escriba los datos correspondientes en los campos. Para obtener más información sobre las descripciones de los campos, consulte la *Ayuda en línea*.

3 Para conectarse a un recurso compartido de archivos remotos, haga clic en **Conectar**. Para conectarse a un recurso compartido de archivos remotos, debe proporcionar la ruta, el nombre de usuario y la contraseña. Si la operación es correcta, se le permite acceder a los medios.

Haga clic en **Desconectar** para desconectarse de un recurso compartido de archivos remotos al que se conectó anteriormente.

Haga clic en **Implementar** para implementar el dispositivo de medios.

NOTA: Antes de hacer clic en el botón Implementar, asegúrese de guardar todos los archivos de trabajo, dado que esta acción reinicia el servidor.

Cuando hace clic en **Implementar**, se ejecutan las siguientes tareas:

- El recurso compartido de archivos remotos se conecta.
- El archivo se selecciona como primer dispositivo de inicio de los servidores.
- El servidor se reinicia.
- Se suministra energía al servidor si está apagado.

Configuración de las opciones de perfil con la replicación de configuración de servidores

La función de replicación de configuración de servidores le permite aplicar todas las opciones de perfil de un servidor especificado a uno o más servidores. Las opciones de perfil que pueden replicarse son las que pueden modificarse y están pensadas para replicarse en servidores. Se muestran los siguientes tres grupos de perfiles de servidores, que pueden replicarse:

- BIOS: este grupo incluye solo los valores del BIOS de un servidor. Estos perfiles se generan desde la CMC para PowerEdge VRTX versión 1.00 y posteriores.
- BIOS e inicio: este grupo incluye los valores del BIOS y de inicio de un servidor. Estos perfiles se generan desde la CMC para PowerEdge VRTX versión 1.00 y posteriores.
- Todas las opciones: esta versión incluye todas las opciones de configuración del servidor y los componentes en ese servidor. Estos perfiles se generan desde
  - CMC para PowerEdge VRTX versión 1.00 y posterior
  - Servidores de 12.ª generación con iDRAC7 1.00.00 o posterior, con Lifecycle Controller 2 versión 1.1 o posterior
  - Servidores de 13.ª generación con iDRAC8 con Lifecycle Controller 2.00.00.00 o posterior

La función de replicación de configuración de servidores admite los servidores iDRAC7 y posteriores. Los servidores RAC de generaciones anteriores se muestran en la lista pero aparecen atenuados en la página principal y no están activados para usar esta función.

Para usar la función de replicación de configuración de servidores:

- Debe tener la versión mínima requerida del iDRAC.
- El servidor debe estar encendido.

Puede:

- Ver la configuración del perfil de un servidor o de un perfil guardado.
- Guardar un perfil de un servidor.
- Aplicar un perfil a otros servidores.
- Importar los perfiles almacenados desde una estación de administración o un recurso compartido de archivos remotos.
- Editar el nombre y la descripción del perfil.
- Exportar los perfiles almacenados a una estación de administración o un recurso compartido de archivos remotos.
- Eliminar perfiles guardados.
- Implementar los perfiles seleccionados en los dispositivos de destino con la opción **Implementación rápida**.
- Mostrar la actividad del registro para las tareas recientes de perfil del servidor.

Acceso a la página Perfiles de servidores

Es posible agregar, administrar y aplicar perfiles de servidores en uno o varios servidores mediante la página **Perfiles de servidores**.

Para acceder a la página **Perfiles de servidores** mediante la interfaz web de la CMC, en el panel izquierdo, vaya a **Descripción general del chasis** > **Descripción general del servidor**. Haga clic en **Configuración** > **Perfiles**. Se muestra la página **Perfiles del servidor**.

Agregar o guardar perfil

Antes de copiar las propiedades de un servidor, primero es necesario capturarlas en un perfil almacenado. Cree un perfil almacenado e ingrese un nombre y una descripción opcional para cada perfil. Puede guardar un máximo de 16 perfiles almacenados en los medios de almacenamiento extendido no volátiles de la CMC.

NOTA: Si está disponible un recurso compartido remoto, puede almacenar un máximo de 100 perfiles utilizando el almacenamiento extendido de la CMC y el recurso compartido remoto. Para obtener más información acerca del recurso compartido remoto, consulte Configuración de un recurso compartido de red mediante la interfaz web de la CMC.

La eliminación o desactivación del soporte de almacenamiento extendido no volátil impide el acceso al perfil almacenado y desactiva la función Clonación de configuración de servidores.

Para agregar o guardar un perfil:

1 Abra la página **Perfiles del servidor**. En la sección **Perfiles del servidor**, haga clic en **Aplicar y guardar perfiles**.

2 Seleccione el servidor desde cuya configuración desee generar el perfil y, a continuación, haga clic en **Guardar perfil**.

Aparece la sección **Guardar perfil**.

3 Seleccione **Almacenamiento extendido** o **Recurso compartido de red** como la ubicación en la que desea guardar el perfil.

NOTA: La opción Recurso compartido de red está activada y los detalles aparecerán en la sección Perfiles almacenados solo si el recurso compartido de red está montado y se puede acceder al mismo. Si el recurso compartido de red no está conectado, configure el recurso compartido de red del chasis. Para configurar el recurso compartido de red, haga clic en Editar en la sección Perfiles almacenados. Para obtener más información acerca de cómo configurar el recurso compartido de red, consulte Configuración de un recurso compartido de red mediante la interfaz web de la CMC.

4 En los campos **Nombre de perfil** y **Descripción**, ingrese el nombre de perfil y la descripción (opcional), y haga clic en **Guardar perfil**.

NOTA: Al guardar un perfil de servidor, se admite el conjunto de caracteres extendidos ASCII estándar. No obstante, no se admiten los siguientes caracteres especiales:

), “, ., *, >, <, \, /, :, |, #, ?, y ,

La CMC se comunica con el LC para obtener la configuración del perfil del servidor disponible y almacenarla como perfil designado.

El indicador de progreso indica que la operación Guardar está en progreso. Una vez que se complete la acción, se visualizará el mensaje "Operación satisfactoria".

NOTA: El proceso de recolección de la configuración se ejecuta en segundo plano. En consecuencia, es posible que el nuevo perfil tarde algunos minutos en visualizarse. Si el nuevo perfil no se visualiza, haga clic en el registro del perfil para ver los errores.

Aplicación de un perfil

La replicación de la configuración de servidores solamente es posible cuando existen perfiles de servidores disponibles como perfiles almacenados en los medios no volátiles de la CMC o almacenados en el recurso compartido remoto. Para iniciar una operación de replicación de configuración de servidores, puede aplicar un perfil almacenado a uno o más servidores.

NOTA: Si el servidor no admite Dell Lifecycle Controller o si el chasis está apagado, no se puede aplicar un perfil al servidor.

Para aplicar un perfil a uno o varios servidores:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Guardar y aplicar perfiles**, seleccione el o los servidores para los que desea aplicar el perfil seleccionado.

Se activará el menú desplegable **Seleccionar perfil**.

NOTA: El menú desplegable Seleccionar perfil muestra todos los perfiles disponibles y clasificados por tipo, incluidos aquellos que se encuentran en el recurso compartido remoto y la tarjeta SD.

2 En el menú desplegable **Seleccionar perfil**, seleccione el perfil que desea aplicar.

Se activa la opción **Aplicar perfil**.

3 Haga clic en **Aplicar perfil**.

Aparece un mensaje de aviso de que al aplicar un nuevo perfil de servidor se sobrescribirá la configuración actual y también se reiniciarán los servidores seleccionados. Se le pide que confirme si desea continuar con la operación.

NOTA: Para realizar operaciones de clonación en servidores, la opción CSIOR debe estar activada para los servidores. Si esta opción está desactivada, aparecerá un mensaje de advertencia para notificar que CSIOR no está activado para los servidores. Para completar la operación de clonación de blade, asegúrese de activar la opción CSIOR en los servidores.

4 Haga clic en **Aceptar** para aplicar el perfil al servidor seleccionado.

El perfil seleccionado se aplica a los servidores, los cuales pueden reiniciarse de inmediato si es necesario. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Importar archivo

Puede importar a la CMC un perfil de servidor almacenado en una estación de administración.

Para importar un perfil almacenado a partir de la CMC:

1 En la página **Perfiles de servidor**, en la sección **Perfiles almacenados**, haga clic en **Importar perfil**.

Aparecerá la sección **Importar perfil de servidor**.

2 Haga clic en **Explorar** para acceder al perfil desde la ubicación requerida y luego haga clic en **Importar perfil**.

Para obtener más información acerca de los campos, consulte la *Ayuda en línea*.

Exportar archivo

Puede exportar un perfil del servidor almacenado a una ruta de acceso a carpeta de archivos especificada en una estación de administración.

Para exportar un perfil almacenado:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Exportar perfil**.

Aparecerá el cuadro de diálogo **Descarga de archivo**, donde se le solicitará que abra o guarde el archivo.

2 Haga clic en **Guardar** o **Abrir** para exportar el perfil en la ubicación requerida.

NOTA: Si el perfil de origen está en la tarjeta SD, aparece un mensaje que le indica que si se exporta el perfil, se perderá la descripción. Presione Aceptar para continuar con la exportación del perfil.

Aparece un mensaje que le solicita que seleccione el destino del archivo:

- local o recurso compartido de red si el archivo de origen está en una tarjeta SD.

NOTA: La opción Recurso compartido de red está activada y los detalles aparecerán en la sección Perfiles almacenados solo si el recurso compartido de red está montado y se puede acceder al mismo. Si el recurso compartido de red no está conectado, configure el recurso compartido de red del chasis. Para configurar el recurso compartido de red, haga clic en Editar en la sección Perfiles almacenados. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web de la CMC.

- Local o tarjeta SD o si el archivo de origen está en el recurso compartido de red.

Para obtener más información acerca de los campos, consulte la *Ayuda en línea*.

3 Seleccione **Local**, **Almacenamiento extendido** o **Recurso compartido de red** como ubicación de destino en función de las opciones que se muestran.

- Si selecciona **Local**, aparecerá un cuadro de diálogo que le permite guardar el perfil en un directorio local.
- Si selecciona **Almacenamiento extendido** o **Recurso compartido de red**, se muestra el cuadro de diálogo **Guardar perfil**.

4 Haga clic en **Guardar perfil** para guardar el perfil en la ubicación seleccionada.

NOTA: La interfaz web de la CMC captura el perfil normal de configuración del servidor (instantánea del servidor), que se puede utilizar para la replicación en un sistema de destino. Sin embargo, algunas configuraciones, como por ejemplo, RAID y los atributos de la identidad no se propagan al nuevo servidor. Para obtener más información sobre los modos exportación alternativo para las configuraciones RAID y los atributos de identidad, consulte el documento técnico, *Clonación de servidores con perfiles de configuración del servidor*, en DellTechCenter.com.

Editar perfil

Puede editar el nombre y la descripción de un perfil de servidor que está almacenado en los medios no volátiles del CMC (tarjeta de SD) o el nombre de un perfil de servidor almacenado en el recurso compartido remoto.

Para editar un perfil almacenado:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Editar perfil**.

Aparecerá la sección **Editar perfil del servidor— <Nombre de perfil>**.

2 Edite el nombre y la descripción del perfil del servidor según sea necesario y luego haga clic en **Editar perfil**.

NOTA: Puede editar la descripción del perfil solamente para los perfiles almacenados en tarjetas SD.

Para obtener más información, consulte la *Ayuda en línea*.

Eliminar perfil

Puede eliminar un perfil del servidor que está almacenado en los medios no volátiles del CMC (tarjeta de SD) o en el recurso compartido de red.

Para eliminar un perfil almacenado:

1 En la página **Perfiles del servidor**, en la sección **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Eliminar perfil**.

Aparecerá un mensaje de aviso donde se indica que al eliminar un perfil se eliminará permanentemente el perfil seleccionado.

2 Haga clic en **Aceptar** para eliminar el perfil seleccionado.

Para obtener más información, consulte la *Ayuda en línea*.

Visualizar configuración de perfil

Para ver la configuración del perfil de un servidor seleccionado, diríjase a la página **Perfiles del servidor**. En la sección **Perfiles del servidor**, haga clic en **Ver** en la columna **Perfil del servidor** para el servidor requerido. Aparece la página **Ver configuración**.

Para obtener más información sobre la configuración visualizada, consulte la *Ayuda en línea*.

NOTA: La función Replicación de configuración de servidores del CMC recupera y muestra los valores de un servidor específico solamente si la opción Recolectar inventario del sistema en el reinicio (CSIOR) se encuentra activada.

Para activar CSIOR en:

- Servidores de 12a generación: después de reiniciar el servidor, cuando el logotipo de la empresa aparece, seleccione F2. En la página **Configuración de iDRAC**, en el panel izquierdo, haga clic en **Lifecycle Controller**, y, a continuación, haga clic en **CSIOR** para activar los cambios.
- Servidores de 13.ª generación: después de reiniciar el servidor, cuando se le solicite, presione F10 para acceder a Dell Lifecycle Controller. Para ir a la página **Inventario de hardware** , haga clica en **Configuración de hardware** > **Inventario de hardware**. En la página **Inventario de hardware** , haga clic en **Recopilar inventario del sistema al reinicio**.

Visualización de la configuración de los perfiles almacenados

Para ver la configuración del perfil de los perfiles de servidores almacenados, vaya a la página **Perfiles del servidor**. En la sección **Perfiles almacenados**, haga clic en **Ver** en la columna **Ver perfil** del perfil de servidor requerido. Aparece la página **Ver configuración**. Para obtener más información sobre la configuración visualizada, consulte la *Ayuda en línea*.

Visualización del registro de perfiles

Para ver el registro de perfiles, en la página **Perfiles del servidor**, consulte la sección **Registro de perfiles reciente**. Esta sección enumera las 10 entradas más recientes del registro de perfiles directamente desde las operaciones de configuración de servidores. Cada entrada del registro muestra la gravedad, la fecha y la hora de envío de la operación de replicación de configuración de servidores y la descripción del mensaje de registro de replicación. Las entradas del registro también están disponibles en el registro del RAC. Para ver el resto de las entradas disponibles, haga clic en **Ir al registro de perfiles**. Aparecerá la página **Registro de perfiles**. Para obtener más información, consulte la *Ayuda en línea*.

Estado de compleción y solución de problemas

Para revisar el estado de compleción de un perfil de BIOS aplicado:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del servidor** > **Configuración** > **Perfiles**.
2. En la página **Perfiles del servidor**, anote el valor de Identificación de trabajo (JID) para el trabajo enviado a partir de la sección **Registro de perfiles reciente**.
3. En el panel izquierdo, haga clic en **Descripción general del servidor** > **Solución de problemas** > **Trabajos de Lifecycle Controller**. Busque la misma identificación de trabajos en la tabla **Trabajos**. Para obtener más información acerca de cómo llevar a cabo trabajos en Lifecycle Controller mediante la CMC, consulte Operaciones de trabajo en Lifecycle Controller.
4. Haga clic en el vínculo **Ver registro** para ver los resultados de *Lclogview* de Lifecycle Controller del iDRAC para el servidor específico.

   Los resultados que se muestren para la finalización o la falla son similares a la información que se muestra en el registro de Lifecycle Controller del iDRAC para el servidor específico.

Implementación rápida de perfiles

La función Implementación rápida le permite asignar un perfil almacenado a una ranura del servidor. Cualquier servidor compatible con la replicación de configuración del servidor insertado en una ranura se configurará con el perfil asignado a dicha ranura. Puede realizar la acción Implementación rápida solamente si la opción **Acción cuando el servidor está insertado** de la página **Implementar el iDRAC** está establecida en la opción **Perfil de servidor** o en la opción **Implementación rápida y perfil del servidor**. Si se selecciona esta opción, se permite aplicar el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis. Para ir a la página **Implementar iDRAC**, seleccione **Descripción general del servidor** > **Configuración** > **iDRAC**. Los perfiles que se pueden implementar se encuentran en la tarjeta SD o en el recurso compartido remoto. Para configurar los perfiles para implementación rápida, debe tener privilegios de **Administrador del chasis**.

NOTA:

Asignación de perfiles del servidor a ranuras

La página **Perfiles del servidor** le permite asignar perfiles a ranuras. Para asignar un perfil a las ranuras del chasis:

1 En la página **Perfiles del servidor**, haga clic en **Perfiles para implementación rápida**.
Aparecerán las asignaciones de perfiles actuales para las ranuras en los cuadros seleccionados en la columna **Asignar perfil**.

NOTA: Puede realizar la acción Implementación rápida solamente si la opción Acción cuando el servidor está insertado de la página Implementar el iDRAC está establecida en Perfil de servidor o en Implementación rápida y luego el perfil del servidor. Si se selecciona esta opción, se permite aplicar el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis.

2 En el menú desplegable, seleccione el perfil que desea asignar a la ranura requerida. Puede seleccionar un perfil para aplicar a varias ranuras.

3 Haga clic en **Asignar perfil**.
El perfil se asigna a las ranuras seleccionadas.

NOTA:

- Una ranura que no tiene ningún perfil asignado se indica mediante el término “Sin perfil seleccionado” que aparece en el cuadro de selección.
- Para eliminar la asignación de un perfil de una o más ranuras, seleccione las ranuras y haga clic en **Quitar asignación**. Aparece un mensaje advirtiéndole que al extraer un perfil de las ranuras se eliminan los valores de configuración del perfil de cualquier servidor insertado en la ranura cuando se activa la función de **Perfiles de implementación rápida**. Haga clic en **Aceptar** para quitar las asignaciones de perfil de almacenamiento.
- Para quitar todas las asignaciones de perfiles de una ranura, seleccione **Sin perfil seleccionado** en el menú desplegable.

NOTA: Cuando se implementa un perfil en un servidor con la función Implementación rápida de perfiles, el progreso y los resultados de la aplicación se conservan en el registro de perfiles.

NOTA:

- Si no se puede acceder al perfil asignado en el recurso compartido de red cuando se inserta un servidor en la ranura, la pantalla LCD muestra un mensaje que indica que el perfil asignado no está disponible para la ranura <X>.
- La opción **Recurso compartido de red** está activada y los detalles aparecerán en la sección **Perfiles almacenados** solo si el recurso compartido de red está montado y se puede acceder al mismo. Si el recurso compartido de red no está conectado, configure el recurso compartido de red del chasis. Para configurar el recurso compartido de red, haga clic en **Editar** en la sección **Perfiles almacenados**. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web de la CMC.

Perfiles de identidad de inicio

Para acceder a la página **Perfiles de identidad de inicio** en la interfaz web de la CMC, en el árbol del sistema, vaya a **Descripción general del chasis** > **Descripción general del servidor**. Haga clic en **Configuración** > **Perfiles**. Se muestra la página **Perfiles del servidor**. En la página **Perfiles del servidor**, haga clic en **Perfiles de identidad de inicio**.

Los perfiles de identidad de inicio contienen la configuración de NIC o FC requerida para iniciar un servidor desde un dispositivo SAN de destino, además de MAC y WWN virtual únicos. Debido a que estos se encuentran disponibles a través de varios chasis mediante los recursos compartidos NFS o CIFS, es posible poner en marcha una identidad rápidamente y de manera remota desde un servidor no funcional en un chasis a un servidor de reserva ubicado en el mismo chasis o en otro, lo que le permite iniciar con el sistema operativo y las aplicaciones del servidor que falló. La principal ventaja de esta función es utilizar el bloque de direcciones MAC virtuales, que es exclusivo y se comparte entre todos los chasis.

Esta función le permite administrar las operaciones de servidores en línea sin intervención física en caso de que el servidor deje de funcionar. Puede realizar las siguientes tareas mediante la función Perfiles de identidad de inicio:

- Configuración inicial
  - Crear un rango de direcciones MAC virtuales. Para crear una dirección MAC, debe tener privilegios de Administrador del servidor y Administrador de configuración del chasis.
  - Guarde plantillas de perfiles de identidad de inicio y personalice los perfiles de identidad de inicio en el recurso compartido de red mediante la edición e incluyendo los parámetros de inicio SAN que utiliza cada servidor.
  - Prepare los servidores que utilizan configuración inicial antes de aplicar sus perfiles de identidad de inicio.
  - Aplique perfiles de identidad de inicio a cada servidor e inícielos desde SAN.
- Configure uno o más servidores de reserva en espera para la recuperación rápida.
  - Prepare los servidores en espera que utilizan configuración inicial antes de aplicar sus perfiles de identidad de inicio.
- Utilice la carga de trabajo de un servidor fallido en un servidor nuevo mediante las siguientes tareas:
  - Borre la identidad de inicio del servidor que no funciona para evitar duplicar las direcciones MAC en caso de que el servidor se recupere.
  - Aplique la identidad de inicio de un servidor fallido a un servidor en espera de repuesto.
  - Inicie el servidor con la nueva configuración de la identidad Inicio para recuperar rápidamente la carga de trabajo.

Cómo guardar perfiles de identidad de inicio

Puede guardar perfiles de identidad de inicio en el recurso compartido de red de la CMC. La cantidad de perfiles que puede almacenar depende de la disponibilidad de las direcciones MAC. Para obtener más información, consulte *Configuración de un recurso compartido de red mediante la interfaz web del CMC*.

Para las tarjetas Emulex Fibre Channel (FC), el atributo **Activar/Desactivar inicio desde SAN** en el ROM de opción está desactivado de forma predeterminada. Active el atributo en el ROM de opción y aplique el perfil de identificación de inicio al servidor para el inicio desde SAN.

Para guardar un perfil, realice las siguientes tareas:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio**, seleccione el servidor que tiene los valores necesarios con los que desea generar el perfil y seleccione FQDD del menú desplegable **FQDD**.

2 Haga clic en **Guardar identidad**. Aparece la sección **Almacenamiento de identidad**.

NOTA: La identidad de inicio se guarda solo si la opción Recurso compartido de red está activada y es accesible, y los detalles se muestran en la sección Perfiles almacenados. Si el recurso compartido de red no está conectado, configure el recurso compartido de red del chasis. Para configurar el recurso compartido de red, haga clic en Editar en la sección Perfiles almacenados. Para obtener más información, consulte *Configuración de un recurso compartido de red mediante la interfaz web del CMC*.

3 En los campos **Nombre de perfil base** y **Número de perfiles**, introduzca el nombre de perfil y el número de perfiles que desee guardar.

NOTA: Al guardar un perfil de identidad de inicio, se admite el conjunto de caracteres extendidos ASCII estándar. No obstante, no se admiten los siguientes caracteres especiales:

), “, ., *, >, <, \, /, :, |, #, ?, y ,

4 Seleccione una dirección MAC para el perfil base del menú desplegable **Dirección MAC virtual** y haga clic en **Guardar perfil**.

La cantidad de plantillas creadas se basa en el número de perfiles que especifique. El CMC se comunica con Lifecycle Controller para obtener la configuración del perfil del servidor disponible y almacenarla como perfil designado. El formato para el archivo de nombre es: <base profile name>_<profile number>_<MAC address>. Por ejemplo: FC630_01_0E0000000000.

El indicador de progreso indica que la operación Guardar está en progreso. Una vez finalizada la acción, aparece el mensaje **Operación exitosa**:

NOTA: El proceso de recolección de la configuración se ejecuta en segundo plano. En consecuencia, es posible que el nuevo perfil tarde algunos minutos en visualizarse. Si el nuevo perfil no se visualiza, haga clic en el registro del perfil para ver los errores.

Aplicación de perfiles de identidad de inicio

Puede aplicar los valores de perfiles de identidad de inicio si estos perfiles están disponibles como perfiles almacenados en el recurso compartido de red. Para iniciar una operación de configuración de identidad de inicio, puede aplicar un perfil almacenado a un único servidor.

NOTA: Si el servidor no admite Lifecycle Controller o si el chasis está apagado, no se puede aplicar un perfil al servidor.

Para aplicar un perfil a un servidor, realice las siguientes tareas:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio**, seleccione el servidor en el que desee aplicar el perfil seleccionado.

Se activará el menú desplegable **Seleccionar perfil**.

NOTA: El menú desplegable Seleccionar perfil muestra todos los perfiles disponibles clasificados por tipo desde el recurso compartido de red.

2 En el menú desplegable **Seleccionar perfil**, seleccione el perfil que desea aplicar.

Se activa la opción **Aplicar perfil**.

3 Haga clic en **Aplicar identidad**.

Aparece un mensaje de aviso de que al aplicar una nueva identidad se sobrescribe la configuración actual y también se reinicia el servidor seleccionado. Se le pide que confirme si desea continuar con la operación.

NOTA: Para realizar operaciones de replicación de la configuración del servidor, la opción CSIOR debe estar activada para los servidores. Si la opción CSIOR está desactivada, se mostrará un mensaje de advertencia que indica que CSIOR no está activada para el servidor. Para completar la operación de replicación de la configuración del servidor, active la opción CSIOR en el servidor.

4 Haga clic en **Aceptar** para aplicar el perfil de identidad de inicio en el servidor seleccionado.

El perfil seleccionado se aplica al servidor y este se reinicia inmediatamente. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

NOTA: Puede aplicar un perfil de identidad de inicio para solo una partición de NIC FQDD en un servidor a la vez. Para aplicar el mismo perfil de identidad de inicio a una partición de NIC FQDD en otro servidor, debe borrarlo del servidor en el que se aplica por primera vez.

Cómo borrar perfiles de identidad de inicio

Antes de aplicar un nuevo perfil de identidad de inicio a un servidor en espera, puede borrar las configuraciones de identidad de inicio existentes de un servidor seleccionado mediante la opción **Borrar identidad** disponible en la interfaz web de la CMC.

Para borrar los perfiles de identidad de inicio:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio**, seleccione el servidor desde el que desea borrar el perfil de identidad de inicio.

NOTA: Esta opción se activa solo si se selecciona alguno de los servidores y si los perfiles de identidad de inicio se aplican a los servidores seleccionados.

2 Haga clic en **Borrar identidad**.

3 Haga clic en **Aceptar** para borrar el perfil de identidad de inicio del servidor seleccionado.

La operación de borrado desactiva la identidad de E/S y de la política de persistencia del servidor. Al finalizar la operación de borrado, el servidor se apaga.

Visualización de perfiles de identidad de inicio almacenados

Para ver los perfiles de identidad de inicio almacenados en el recurso compartido de red, vaya a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Perfiles almacenados**, seleccione el perfil y haga clic en **Ver** en la columna **Ver perfil**. Aparece la página **Ver configuración**. Para obtener más información sobre la configuración visualizada, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Cómo importar perfiles de identidad de inicio

Puede importar perfiles de identidad de inicio almacenados en la estación de administración al recurso compartido de red.

Para importar un perfil almacenado al recurso compartido de red desde la estación de administración, realice las siguientes tareas:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Perfiles almacenados**, haga clic en **Importar perfil**.

Se mostrará la sección **Importar perfil**.

2 Haga clic en **Explorar** para acceder al perfil desde la ubicación requerida y luego haga clic en **Importar perfil**.

Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Cómo exportar perfiles de identidad de inicio

Puede exportar perfiles de identidad de inicio guardados en el recurso compartido de red a una ruta de acceso especificada en una estación de administración.

Para exportar un perfil almacenado, realice las siguientes tareas:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Perfiles almacenados**, seleccione el perfil necesario y haga clic en **Exportar perfil**.

Aparecerá el cuadro de diálogo **Descarga de archivo**, donde se le solicitará que abra o guarde el archivo.

2 Haga clic en **Guardar** o **Abrir** para exportar el perfil en la ubicación requerida.

Eliminación de perfiles de identidad de inicio

Puede eliminar un perfil de identidad de inicio almacenado en el recurso compartido de red.

Para eliminar un perfil almacenado, realice las siguientes tareas:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Perfiles almacenados**, seleccione el perfil necesario y haga clic en **Eliminar perfil**.

Aparecerá un mensaje de advertencia donde se indica que al eliminar un perfil se eliminará permanentemente el perfil seleccionado.

2 Haga clic en **Aceptar** para eliminar el perfil seleccionado.

Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Administración de bloque de direcciones MAC virtuales

Puede crear, agregar, quitar y desactivar las direcciones MAC mediante la **Administración de bloque de direcciones MAC virtuales**. En el bloque de direcciones MAC virtuales sólo puede utilizar direcciones MAC de unidifusión. En la CMC se permiten los siguientes rangos de dirección MAC.

- 02:00:00:00:00:00 - F2:FF:FF:FF:FF:FF
- 06:00:00:00:00:00 - F6:FF:FF:FF:FF:FF
- 0A:00:00:00:00:00 - FA:FF:FF:FF:FF:FF
- 0E:00:00:00:00:00 - FE:FF:FF:FF:FF:FF

Para ver la opción **Administrar la dirección MAC virtual**, por la interfaz web de la CMC, en el árbol del sistema, vaya a **Descripción general del chasis** > **Descripción general del servidor**. Haga clic en **Configuración** > **Perfiles** > **Perfiles de identidad de inicio**. Se muestra la sección **Administración de bloque de direcciones MAC virtuales**.

NOTA: Las direcciones MAC virtuales se administran en el archivo vmacdb.xml en el recurso compartido de red. Un archivo de bloqueo oculto (.vmacdb.lock) se agrega y se retira del recurso compartido de red para serializar las operaciones de identidad de inicio de varios chasis.

Creación de bloque de MAC

Puede crear bloque de MAC en la red mediante la opción **Administrar bloque de direcciones MAC virtuales** disponible en la interfaz web de la CMC.

NOTA: La sección Creación de bloque de MAC solo se muestra si la base de datos de direcciones MAC (vmacdb.xml) no está disponible en el recurso compartido de red. En este caso, se desactivan las opciones Agregar dirección MAC y Eliminar dirección MAC.

Para crear un bloque de MAC:

1 Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Administrar bloque de direcciones MAC virtuales**.

2 Introduzca la dirección MAC de inicio de el bloque de direcciones MAC en el campo **Dirección MAC de inicio**.

3 Introduzca el recuento de direcciones MAC en el campo **Número de direcciones MAC**.

4 Haga clic en **Crear bloque de MAC** para crear el bloque de direcciones MAC.

Una vez creada la base de datos de direcciones MAC en el recurso compartido de red, **Administrar bloque de direcciones MAC virtuales** muestra la lista y el estado de las direcciones MAC almacenadas en el recurso compartido de red. Esta sección ahora permite agregar o quitar direcciones MAC desde el bloque de direcciones MAC.

Cómo agregar direcciones MAC

Puede agregar un rango de direcciones MAC en el recurso compartido de red mediante la opción **Agregar direcciones MAC** disponible en la interfaz web de la CMC.

NOTA: No puede agregar una dirección MAC que ya existe en el bloque de direcciones MAC. Se muestra un error que indica que la dirección MAC agregada recientemente ya existe en el bloque.

Para agregar direcciones MAC en el recurso compartido de red:

1. Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Administrar bloque de direcciones MAC virtuales**, haga clic en **Agregar direcciones MAC**.
2. Introduzca la dirección MAC de inicio de el bloque de direcciones MAC en el campo **Dirección MAC de inicio**.
3. Introduzca el recuento de las direcciones MAC que desea agregar en el campo **Número de direcciones MAC**.

   Los valores válidos son de 1 a 3000.
4. Haga clic en **Aceptar** para agregar direcciones MAC.

   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

   Para obtener más información, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

Eliminación de direcciones MAC

Puede eliminar un rango de direcciones MAC del recurso compartido de red mediante la opción **Eliminar direcciones MAC** disponible en la interfaz web de la CMC.

NOTA: No puede eliminar direcciones MAC que estén activas en el nodo o que estén asignadas a un perfil.

Para eliminar direcciones MAC del recurso compartido de red:

1. Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Administrar bloque de direcciones MAC virtuales**, haga clic en **Eliminar direcciones MAC**.
2. Introduzca la dirección MAC de inicio de el bloque de direcciones MAC en el campo **Dirección MAC de inicio**.
3. Introduzca el recuento de las direcciones MAC que desea eliminar en el campo **Número de direcciones MAC**.
4. Haga clic en **Aceptar** para eliminar direcciones MAC.

Desactivación de direcciones MAC

Puede desactivar las direcciones MAC activas mediante la opción **Desactivar direcciones MAC** en la interfaz web de la CMC.

NOTA: Utilice la opción Desactivar direcciones MAC solo si el servidor no responde a la acción Borrar identidad o la dirección MAC no se utiliza en ningún servidor.

Para eliminar direcciones MAC del recurso compartido de red:

1. Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles de identidad de inicio** > **Administrar bloque de direcciones MAC virtuales**, seleccione las direcciones MAC activas que desea desactivar.
2. Haga clic en **Desactivar direcciones MAC**.

Inicio del iDRAC mediante el inicio de sesión único

La CMC proporciona una administración limitada de los componentes individuales del chasis, como los servidores. Para una administración completa de estos componentes individuales, la CMC proporciona un punto de inicio para la interfaz basada en la web de la controladora de administración del servidor (iDRAC).

Un usuario puede iniciar la interfaz web del iDRAC sin tener que iniciar sesión por segunda vez, ya que esta función utiliza el inicio de sesión único. Las políticas de inicio de sesión único son:

- Un usuario de la CMC con privilegio de administración del servidor inicia sesión automáticamente en iDRAC mediante el inicio de sesión único. Una vez que se encuentre en el sitio del iDRAC, a este usuario se le otorgarán privilegios de administrador automáticamente. Esto sucede incluso cuando el mismo usuario no dispone de una cuenta en el iDRAC o la cuenta no tiene privilegios de administrador.
- Un usuario de la CMC que **NO** tiene privilegios de administrador del servidor, pero tiene la misma cuenta en el iDRAC, iniciará sesión automáticamente en iDRAC mediante el inicio de sesión único. Una vez que este usuario se encuentre en el sitio del iDRAC, se le otorgarán privilegios que fueron creados para la cuenta del iDRAC.
- Un usuario de la CMC que no tiene privilegios de administrador del servidor ni la misma cuenta en el iDRAC, no podrá iniciar sesión automáticamente en iDRAC mediante el inicio de sesión único. Este usuario será dirigido a la página de inicio de sesión del iDRAC al hacer clic en **Iniciar la interfaz gráfica de usuario del iDRAC**.

NOTA: En este contexto, el término "la misma cuenta" significa que el usuario tiene el mismo nombre de inicio de sesión con la misma contraseña para la CMC como para el iDRAC. Se considerará que el usuario que tenga el mismo nombre de inicio de sesión, aunque una contraseña diferente, tiene la misma cuenta.

NOTA: Se puede pedir a los usuarios que inicien sesión en el iDRAC (consulte la política de inicio de sesión único en la tercera viñeta anterior).

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

Si hace clic en **Iniciar la interfaz gráfica de usuario del iDRAC**, podrá aparecer una página de error, si:

- se desmonta el servidor del chasis.
- se cambia la dirección IP del iDRAC
- la conexión de red del iDRAC tiene algún problema.

En MCM, al iniciar la interfaz web del iDRAC desde un chasis miembro, las credenciales de usuario del chasis principal y los chasis miembros deben ser las mismas. De lo contrario, la sesión actual del chasis miembro se anula y se visualiza la página de inicio de sesión del chasis miembro.

Inicio del iDRAC desde la página Estado del servidor

Para iniciar la consola de administración del iDRAC de un servidor individual:

1 En el panel izquierdo, expanda la **Descripción general del servidor**. Los cuatro servidores aparecen en la lista expandida **Descripción general de servidores**.

2 Haga clic en el servidor para el cual desea iniciar la interfaz web del iDRAC.

3 En la página **Estado de los servidores**, haga clic en **Iniciar el iDRAC**.

Se muestra la interfaz web del iDRAC. Para obtener más información sobre las descripciones de los campos, consulte la *Ayuda en línea*.

Inicio del iDRAC desde la página Estado de los servidores

Para iniciar la consola de administración del iDRAC desde la página **Estado de los servidores**, realice estos pasos:

1 En el panel izquierdo, haga clic en **Descripción general del servidor**.
2 En la página **Estado de los servidores**, haga clic en **Iniciar el iDRAC** para el servidor en el que desea iniciar la interfaz web del iDRAC.

Inicio de la consola remota

Es posible iniciar una sesión de KVM (teclado, video y mouse) directamente en el servidor. La función de consola remota solo se admite cuando se cumplen todas las siguientes condiciones:

- El chasis está encendido.
- Servidores que admiten iDRAC7 y iDRAC8.
- La interfaz de LAN en el servidor está activada.
- El sistema host está instalado con JRE (Java Runtime Environment) 6 Update 16 o superior.
- El explorador del sistema host admite el uso de ventanas emergentes (el bloqueo de ventanas emergentes está desactivado).

La consola remota también se puede iniciar desde la interfaz web del iDRAC. Para obtener más información, consulte la *Guía del usuario del iDRAC* disponible en www.dell.com/support/manuals.

Inicio de la consola remota desde la página Condición del chasis

Para iniciar una consola remota desde la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, haga clic en **Propiedades**.
2 En la página **Condición del chasis**, haga clic en el servidor especificado en el gráfico del chasis.
3 En la sección **Vínculos rápidos**, haga clic en el vínculo **Consola remota** para iniciar la consola remota.

Inicio de la consola remota desde la página Estado del servidor

Para iniciar la consola remota de un servidor individual:

1 En el panel izquierdo, expanda **Descripción general del servidor**. Los cuatro servidores aparecerán en la lista de servidores expandidos.
2 Haga clic en el servidor donde desea ejecutar la consola remota.
3 En la página **Estado del servidor**, haga clic en **Iniciar la consola remota**.

Inicio de la consola remota desde la página Estado de los servidores

Para iniciar la consola remota desde la página **Estado de los servidores**:

1 En el panel izquierdo, vaya a **Descripción general del servidor** y haga clic en **Propiedades** > **Estado**. Aparecerá la página **Estado de los servidores**.
2 Haga clic en **Iniciar la consola remota** para el servidor necesario.

8

Configuración del CMC para enviar alertas

Es posible configurar alertas y acciones para ciertos sucesos que se producen en el chasis. Se genera un suceso cuando el estado de un dispositivo o servicio ha cambiado o cuando se detecta una condición de error. Si un suceso coincide con un filtro de sucesos y ha configurado este filtro para que genere un mensaje de alerta (alerta por correo electrónico o de captura de SNMP), entonces se envía una alerta a uno o varios de los destinos configurados, como dirección de correo electrónico, dirección IP o servidor externo.

Para configurar la CMC para enviar alertas:

1 Activa la opción **Alertas de sucesos del chasis**.
2 Opcionalmente, puede filtrar las alertas en función de la categoría o la gravedad.
3 Configure los valores de la alerta por correo electrónico o la captura SNMP.
4 Active las alertas de sucesos del chasis para enviar una alerta por correo electrónico o capturas SNMP a los destinos configurados.

Temas:

Activación o desactivación de alertas

Para enviar alertas a los destinos configurados, debe activar la opción de alerta global. Esta propiedad anula la configuración de la alerta individual.

Asegúrese de que el SNMP o los destinos de alerta por correo electrónico estén configurados para recibir las alertas.

Activación o desactivación de alertas mediante la interfaz web del CMC

Para activar o desactivar la generación de alertas:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Alertas**.
2 En la página **Sucesos del chasis**, en la sección **Activación de alertas del chasis**, seleccione la opción **Activar alertas de sucesos del chasis** para habilitar o borrar la opción para desactivar la alerta.
3 Para guardar la configuración, haga clic en **Aplicar**.

Filtrado de alertas

Es posible filtrar las alertas por categoría y gravedad.

Filtrado de alertas mediante la interfaz web de CMC

Para filtrar las alertas según su categoría y gravedad:

NOTA: Para aplicar los cambios en la configuración de los sucesos del chasis, es necesario tener el privilegio de configuración de alertas.

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Alertas**.
2 En la página **Sucesos del chasis**, en la sección **Filtro de alertas**, seleccione una o varias de las siguientes categorías:
   - **Condición del sistema**
   - **Almacenamiento**
   - **Configuración**
   - **Auditorías**
   - **Actualizaciones**
3 Seleccione uno o más de los niveles de gravedad siguientes:
   - **Crítico**
   - **Aviso**
   - **Informativo**

   En la sección **Alertas supervisadas** se muestran los resultados en función de la categoría y la gravedad seleccionadas. Para obtener información acerca de las descripciones de los campos en esta página, consulte la *Ayuda en línea*.
4 Haga clic en **Aplicar**.

Configuración de alertas de suceso mediante RACADM

Para establecer alertas de suceso, utilice el comando `eventfilters`. Para obtener más información, consulte la *Guía de referencia sobre la línea de comando RACADM de Chassis Management Controller para PowerEdge VRTX* que está disponible en**dell.com/support/manuals**.

Configuración de destinos de alerta

La estación de administración utiliza el protocolo simple de administración de red (SNMP) para recibir datos de la CMC.

Es posible configurar destinos de alerta IPv4 e IPv6, valores de correo electrónico y valores del servidor SMTP y después probar la configuración.

Antes de configurar los valores de la alerta por correo electrónico o la captura SNMP, asegúrese de tener el privilegio de Administrador de configuración del chasis.

Configuración de destinos de alerta de las capturas SNMP

Es posible configurar las direcciones IPv6 o IPv4 para la recepción de capturas SNMP.

Configuración de destinos de alerta de las capturas SNMP mediante la interfaz web del CMC

Para configurar los valores de destino de alerta IPv4 o IPv6 mediante la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Alertas** > **Valores de captura**.
2 En la página **Destinos de alerta de sucesos del chasis**, escriba lo siguiente:
   - En el campo **Destino**, escriba una dirección IP válida. Se utiliza el formato IPv4 de cuatro números con puntos intermedios, la notación de dirección IPv6 estándar o FQDN. Por ejemplo: **123.123.123.123**, **2001:db8:85a3::8a2e:370:7334** o **dell.com**.

Elija un formato que sea consistente con la infraestructura o la tecnología de red. La función Probar captura no puede detectar las elecciones incorrectas en función de la configuración de red actual (por ejemplo, el uso de un destino IPv6 en un entorno exclusivamente de IPv4).

- En el campo **Cadena de comunidad**, especifique un nombre de comunidad válida a la que pertenezca la estación de administración de destino.

  Esta cadena de comunidad difiere de la cadena de comunidad que aparece en la página **Descripción general del chasis** > **Red** > **Servicios**. La cadena de comunidad de capturas SNMP es la comunidad que CMC utiliza para las capturas de salida destinadas a las estaciones de administración. La cadena de comunidad de la página **Descripción general del chasis** > **Red** > **Servicios** es la cadena de comunidad que las estaciones de administración utilizan para consultar el daemon SNMP en la CMC.

- En **Activada**, seleccione la opción correspondiente a la dirección IP de destino para activar la dirección IP de forma que reciba las capturas. Es posible especificar hasta cuatro direcciones IP.

3 Haga clic en **Aplicar** para guardar la configuración.

4 Para probar si la dirección IP puede recibir las capturas SNMP, haga clic en **Enviar** en la columna **Probar captura SNMP**.

Se configurarán los destinos de alerta IP.

Configuración de destinos de alerta de las capturas SNMP mediante RACADM

Para configurar los destinos de alerta IP mediante RACADM:

1 Abra una consola de texto de serie/Telnet/SSH en la CMC e inicie sesión.

NOTA: Solo puede configurarse una máscara de filtro para las alertas por correo electrónico y SNMP. Si ya se ha seleccionado la máscara de filtro, no realice la tarea 2 y vaya al paso 3.

2 Active la generación de alertas:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3 Especifique los filtros de sucesos al ejecutar el comando `racadm eventfilters set`.

a Para borrar todas las configuraciones de alertas disponibles, ejecute el siguiente comando: `racadm eventfilters set -c cmc.alert.all -n none`

b Configure con gravedad como parámetro . Por ejemplo, todos los sucesos informativos en la categoría almacenamiento tienen asignado poweroff como acción y correo electrónico y SNMP como notificaciones: `racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`

c Configurar mediante la subcategoría como un parámetro. Por ejemplo, todas las configuraciones bajo la subcategoría licensing en la categoría audit tienen asignado poweroff como acción y todas las notificaciones están activadas: `racadm eventfilters set -c cmc.alert.audit.lic -n all`

d Configure mediante la subcategoría y la gravedad como parámetros. Por ejemplo, todos los sucesos de información bajo la subcategoría licensing en la categoría audit tienen asignado poweroff como acción y todas las notificaciones están desactivadas: `racadm eventfilters set -c cmc.alert.audit.lic.info -n none`

4 Active las alertas de capturas:

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
```

donde `<index>` es un valor entre 1-4. La CMC usa el número de índice para distinguir hasta cuatro destinos configurables para las alertas de capturas. Los destinos se pueden especificar como direcciones numéricas con el formato apropiado (IPv6 o IPv4) o como nombres de dominio completamente calificados (FQDN).

5 Especifique una dirección IP de destino para recibir la alerta de capturas:

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
```

donde `<IP address>` es un destino válido e `<index>` es el valor de índice que se especificó en el paso 4.

6 Especifique el nombre de comunidad:

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i <index>
```

donde `<community name>` es la comunidad SNMP a la que pertenece el chasis e `<index>` es el valor de índice que se especificó en los pasos 4 y 5.

Puede configurar hasta cuatro destinos para recibir alertas de capturas. Para agregar más destinos, realice las tareas de los pasos 2 a 6.

NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores existentes configurados para el índice especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba `racadm getconfig -g cfgTraps -i <index>`. Si el índice está configurado, aparecerán los valores para los objetos cfgTrapsAlertDestIPAddr y cfgTrapsCommunityName.

7 Para probar cuál es el destino de las alertas de una captura de sucesos, escriba:

```
racadm testtrap -i <index>
```

donde `<index>` es un valor de 1 a 4 que representa el destino de alerta que desea probar.

Si no está seguro acerca del número de índice, ejecute el siguiente comando:

```
racadm getconfig -g cfgTraps -i <index>
```

Configuración de los valores de alertas por correo electrónico

Cuando el CMC detecta un suceso del chasis, como una advertencia del entorno o la falla de un componente, se puede configurar para enviar una alerta por correo electrónico a una o más direcciones de correo electrónico.

Configure el servidor de correo electrónico SMTP para aceptar correos electrónicos retransmitidos de la dirección IP de la CMC, una función que normalmente está desactivada en la mayoría de los servidores de correo electrónico por motivos de seguridad. Para obtener instrucciones acerca de cómo realizarlo de forma segura, consulte la documentación incluida con el servidor SMTP.

NOTA: Si el servidor de correo es Microsoft Exchange Server 2007, compruebe que el nombre de dominio de iDRAC está configurado para que el servidor de correo reciba alertas por correo electrónico desde iDRAC.

NOTA: Las alertas por correo electrónico admiten direcciones IPv4 e IPv6. El nombre de dominio DNS de DRAC se debe especificar mediante IPv6.

Si su red tiene un servidor SMTP que envía y renueva asignaciones de direcciones de IP en forma periódica y las direcciones son diferentes, habrá un plazo en el que la configuración de esta propiedad no funcionará debido al cambio en la dirección de IP especificada del servidor SMTP. En estos casos, use el nombre DNS.

Configuración de los valores de alerta por correo electrónico mediante la interfaz web del CMC

Para configurar los valores de alerta por correo electrónico mediante la interfaz web:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Alertas** > **Valores de alerta de correo electrónico**.

2 Especifique la configuración del servidor de correo electrónico SMTP y las direcciones de correo electrónico para recibir alertas. Para obtener más información sobre las descripciones de los campos, consulte la *Ayuda en línea*.

3 Haga clic en **Aplicar** para guardar la configuración.

4 Haga clic en **Enviar** en la sección **Correo electrónico de prueba** para enviar un correo electrónico de prueba al destino de alerta por correo electrónico especificado.

Configuración de los valores de alerta por correo electrónico mediante RACADM

Para enviar un correo electrónico de prueba a un destino de alerta por correo electrónico mediante RACADM:

1 Abra una consola de texto de serie/Telnet/SSH en la CMC e inicie sesión.

2 Active la generación de alertas:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

NOTA: Solo puede configurarse una máscara de filtro mediante las alertas por correo electrónico y SNMP. Si ya configuró una máscara de filtro, no ejecute la tarea del paso 3.

3 Especifique los sucesos para los que se deben generar alertas:

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

donde `<mask value>` es un valor hexadecimal entre 0x0 y 0xffffffff, y debe expresarse con la caracteres iniciales 0x. En la tabla Máscaras de filtro para capturas de sucesos se proporcionan máscaras de filtro para cada tipo de suceso. Para obtener instrucciones acerca de la forma de calcular el valor hexadecimal para la máscara de filtro que desea activar, consulte el paso 3 en Configuración de destinos de alerta de las capturas SNMP mediante RACADM.

4 Active la generación de alertas por correo electrónico:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
```

donde `<index>` es un valor entre 1-4. La CMC usa el número de índice para distinguir hasta cuatro direcciones de correo electrónico de destino que pueden configurarse.

5 Especifique una dirección de correo electrónico de destino para recibir las alertas por correo electrónico:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i <index>
```

donde `<email address>` es una dirección de correo electrónico válida e `<index>` es el valor del índice que se especificó en el paso 4.

6 Especifique el nombre de la persona que recibirá la alerta por correo electrónico:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i <index>
```

donde `<email name>` es el nombre de la persona o grupo que recibirá la alerta por correo electrónico, e `<index>` es el valor de índice especificado en el paso 4 y el paso 5. El nombre de correo electrónico puede contener hasta 32 caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.

7 Configure el host SMTP:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
```

donde `host.domain` es el FQDN.

Puede configurar hasta cuatro direcciones de correo electrónico de destino para recibir alertas por correo electrónico. Para agregar más direcciones de correo electrónico, ejecute las tareas de los pasos 2 a 6.

NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores existentes configurados para el índice que se ha especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba `racadm getconfig -g cfgEmailAlert – I <index>`. Si el índice está configurado, aparecerán los valores para los objetos cfgEmailAlertAddress y cfgEmailAlertEmailName.

Para obtener más información, consulte la *Guía de referencia sobre la línea de comando RACADM de Chassis Management Controller para PowerEdge VRTX* que está disponible en **dell.com/support/manuals**.

9

Configuración de cuentas de usuario y privilegios

Es posible configurar las cuentas de usuario con privilegios específicos (autoridad basada en funciones) para administrar el sistema mediante la CMC y garantizar la seguridad del mismo. De manera predeterminada, la CMC está configurada con una cuenta de administrador local. El nombre de usuario predeterminado es `root` y la contraseña es `calvin`. Como administrador, es posible configurar cuentas de usuario para permitir a otros usuarios obtener acceso a la CMC.

Es posible configurar hasta 16 usuarios locales o utilizar servicios de directorio, como Microsoft Active Directory o LDAP, para configurar cuentas de usuario adicionales. El uso de un servicio de directorio proporciona una ubicación central para administrar las cuentas de usuario autorizadas.

La CMC admite el acceso basado en funciones para los usuarios con un conjunto de privilegios asociados. Las funciones son: administrador, operador, solo lectura o ninguno. El rol define los privilegios máximos disponibles.

Temas:

Tipos de usuarios

Hay dos tipos de usuarios:

- Usuarios de la CMC o usuarios del chasis
- Usuarios del iDRAC o usuarios del servidor (dado que el iDRAC reside en un servidor)

Los usuarios del iDRAC y de la CMC pueden ser usuarios locales o usuarios del servicio de directorio.

Excepto cuando un usuario de la CMC tenga privilegios de **Administrador del servidor**, los privilegios otorgados a los usuarios de la CMC no se transfieren automáticamente al mismo usuario en un servidor, ya que los usuarios del servidor se crean independientemente de los usuarios de la CMC. En otras palabras, los usuarios de Active Directory de la CMC y los usuarios de Active Directory del iDRAC residen en dos ramas diferentes del árbol de Active Directory. Para crear un usuario del servidor local, los Usuarios de configuración deben conectarse directamente al servidor. Estos Usuarios de configuración no pueden crear un usuario de servidor desde la CMC ni viceversa. Esta regla protege la seguridad y la integridad de los servidores.

Tabla 20. Tipos de usuarios

Privilegio	Descripción
Usuario con acceso a la CMC	El usuario puede iniciar sesión en la CMC y ver todos los datos de la CMC, pero no puede agregar o modificar datos ni ejecutar comandos. Es posible que un usuario tenga otros privilegios sin el privilegio de Usuario con acceso a la CMC. Esta función es útil cuando a un usuario no se le permite iniciar sesión temporalmente. Cuando el privilegio de Usuario con

Privilegio	Descripción
	acceso a la CMC de ese usuario se restablece, el usuario conserva todos los demás privilegios otorgados anteriormente.
Administrador de configuración del chasis	El usuario puede agregar o cambiar los datos que: • Identifican el chasis, como el nombre y la ubicación del chasis. • Están asignados específicamente al chasis, como el modo IP (estático o DHCP), la dirección IP estática, la puerta de enlace estática y la máscara de subred estática. • Brindan servicios al chasis, como la fecha y la hora, la actualización de firmware y el restablecimiento de la CMC. • Se relacionan con el chasis, como el nombre de ranura y la prioridad de ranura. Aunque estas propiedades se aplican a los servidores, se trata estrictamente de propiedades del chasis que se relacionan con las ranuras y no con los propios servidores. Por este motivo, los nombres de ranura y las prioridades de ranura se pueden agregar o cambiar sin importar si los servidores están presentes en las ranuras o no. Cuando se mueve un servidor a un chasis diferente, este hereda el nombre y la prioridad asignados a la ranura que ocupa en el chasis nuevo. La prioridad y el nombre de ranura anteriores se conservarán en el chasis anterior. **NOTA: Los usuarios de la CMC que tienen el privilegio de Administrador de configuración del chasis pueden configurar los valores de alimentación. Sin embargo, el privilegio de Administrador de control del chasis es necesario para realizar operaciones de alimentación del chasis, como el encendido, el apagado y el ciclo de encendido.**
Administrador de configuración de usuarios	El usuario puede: • Agregar un nuevo usuario. • Cambiar la contraseña de un usuario. • Cambiar los privilegios de un usuario. • Activar o desactivar el privilegio de inicio de sesión de un usuario pero conservar el nombre y otros privilegios del usuario en la base de datos.
Administrador de borrado de registros	El usuario puede borrar los registros de hardware y de la CMC.
Administrador de control del chasis (comandos de alimentación)	Los usuarios de la CMC que tienen el privilegio de **Administrador de alimentación del chasis** pueden realizar todas las operaciones relacionadas con la alimentación. Pueden controlar las operaciones de alimentación del chasis, incluso el encendido, el apagado y el ciclo de encendido. **NOTA: Para configurar los valores de alimentación, es necesario el privilegio de Administrador de configuración del chasis.**
Administrador del servidor	Se trata de un privilegio general que otorga al usuario de la CMC todos los derechos para realizar cualquier operación en los servidores que estén presentes en el chasis. Cuando un usuario con el privilegio de **Administrador del servidor** genera una acción que se debe realizar en un servidor, el firmware de la CMC envía el comando al servidor de destino sin verificar los privilegios del usuario en el servidor. Es decir, el privilegio de **Administrador del servidor** anula la falta de privilegios de administrador en el servidor. Sin el privilegio de **Server Administrator**, los usuarios que se hayan creado en el chasis solo pueden ejecutar un comando en un servidor cuando se cumplan todas las condiciones siguientes: • El mismo nombre de usuario existe en el servidor. • El mismo nombre de usuario debe tener la misma contraseña en el servidor. • El usuario debe tener privilegios para ejecutar el comando. Cuando un usuario de la CMC que no tiene privilegios de **Administrador del servidor** genera una acción que se debe realizar en un servidor, la CMC envía un comando al servidor de destino con el nombre de inicio de sesión y la contraseña del usuario. Si el usuario no existe en el servidor o si la contraseña no coincide, se negará al usuario la capacidad de ejecutar la acción.

Privilegio	Descripción
	Si el usuario existe en el servidor de destino y la contraseña coincide, el servidor responderá con los privilegios que se le otorgaron al usuario en el servidor. En función de los privilegios que se tengan en el servidor, el firmware de la CMC decidirá si el usuario tiene derecho de ejecutar la acción. A continuación, se muestran los privilegios y las acciones en el servidor a los que tiene derecho el Administrador del servidor. Estos derechos se aplican solamente cuando el usuario del chasis no tiene el privilegio administrativo del servidor en el chasis. Administrador de configuración del servidor: • Establecer dirección IP • Establecer puerta de enlace • Establecer máscara de subred • Establecer primer dispositivo de inicio Configurar usuarios: • Establecer contraseña raíz del iDRAC • Restablecimiento de iDRAC Administrador de control del servidor: • Encendido • Apagado • Ciclo de encendido • Apagado ordenado • Reinicio del servidor
Usuario de alertas de prueba	El usuario puede enviar mensajes de alerta de prueba.
Administrador de comandos de depuración	El usuario puede ejecutar comandos de diagnóstico del sistema.
Administrador de red Fabric A	El usuario puede definir y configurar el módulo de E/S de la red Fabric A.
Administrador de red Fabric B	El usuario puede definir y configurar la red Fabric B que corresponde a la primera tarjeta mezzanine de los servidores y está conectada al circuito de la red Fabric B en el subsistema PCIe compartido en la placa principal.
Administrador de red Fabric C	El usuario puede definir y configurar la red Fabric C que corresponde a la segunda tarjeta mezzanine de los servidores y está conectada al circuito de la red Fabric C en el subsistema PCIe compartido en la placa principal.

Los grupos de usuarios del CMC proporcionan una serie de grupos de usuarios que tienen privilegios de usuario previamente asignados.

NOTA: Si selecciona Administrador, Usuario avanzado o Usuario invitado y, a continuación, agrega o elimina un privilegio del conjunto predefinido, la opción Grupo de la CMC cambia automáticamente a Personalizado.

Tabla 21. Privilegios del grupo de la CMC

Grupo de usuarios	Privilegios otorgados
Administrador	• Usuario con acceso a la CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador del servidor • Usuario de alertas de prueba

Grupo de usuarios	Privilegios otorgados
	• Administrador de comandos de depuración • Administrador de red Fabric A
Usuario avanzado	• Inicio de sesión • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Administrador del servidor • Usuario de alertas de prueba • Administrador de red Fabric A
Usuario invitado	Inicio de sesión
Personalizado	Seleccione cualquier combinación de los siguientes permisos: • Usuario con acceso a la CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Administrador del servidor • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A
Ninguno	Sin permisos asignados

Tabla 22. Comparación de los privilegios entre administradores, usuarios avanzados y usuarios invitados de la CMC

Conjunto de privilegios	Permisos de administrador	Permisos de usuario avanzado	Permisos de usuario invitado
Usuario con acceso a la CMC	Sí	Sí	Sí
Administrador de configuración del chasis	Sí	No	No
Administrador de configuración de usuarios	Sí	No	No
Administrador de borrado de registros	Sí	Sí	No
Administrador de control del chasis (comandos de alimentación)	Sí	Sí	No
Administrador del servidor	Sí	Sí	No
Usuario de alertas de prueba	Sí	Sí	No
Administrador de comandos de depuración	Sí	No	No
Administrador de red Fabric A	Sí	Sí	No

Modificación de la configuración de cuentas raíz de administración para usuarios

Para una mayor seguridad, se recomienda cambiar la contraseña predeterminada de la cuenta root (Usuario 1). La cuenta raíz es la cuenta de administración predeterminada que se envía con la CMC.

Para cambiar la contraseña predeterminada para la cuenta raíz:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, en **Autentificación de usuario**.
2 En la página **Usuarios**, en la columna **ID de usuario**, haga clic en **1**.

NOTA: La ID de usuario 1 es la cuenta de usuario raíz que se envía con la CMC. Este valor no se puede modificar.

3 En la página **Configuración de usuario**, seleccione la opción **Cambiar contraseña**.
4 Escriba la nueva contraseña en el campo **Contraseña** y, a continuación, escriba la misma contraseña en **Confirmar contraseña**.
5 Haga clic en **Aplicar**. La contraseña se cambia por la ID de usuario **1**.

Configuración de usuarios locales

Es posible configurar hasta 16 usuarios locales en la CMC con privilegios de acceso específicos. Antes de crear un usuario local para la CMC, compruebe si existen usuarios actuales. Puede establecer nombres de usuario, contraseñas y funciones con los privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar mediante cualquiera de las interfaces seguras de la CMC (es decir, la interfaz web, RACADM o WS-MAN).

Configuración de los usuarios locales con la interfaz web del CMC

NOTA: Es necesario contar con el permiso Configurar usuarios para poder crear un usuario de la CMC.

Para agregar y configurar usuarios locales en la CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, en **Autentificación de usuario**.
2 En la página **Usuarios locales**, en la columna **ID de usuario**, haga clic en un número de ID de usuario. Se muestra la página **Configuración de usuario**.

NOTA: Identificación de usuario 1 es la cuenta de usuario raíz que se envía con una CMC. Este valor no se puede modificar.

3 Active la identificación de usuario y especifique el nombre de usuario, la contraseña y los privilegios de acceso de usuario. Para obtener más información sobre estas opciones, consulte *Online Help* (Ayuda en línea).
4 Haga clic en **Aplicar**. El usuario se crea con los privilegios necesarios.

Configuración de los usuarios locales mediante RACADM

NOTA: Se debe haber iniciado sesión como usuario `root` para ejecutar los comandos RACADM en un sistema remoto con Linux.

Es posible configurar hasta 16 usuarios en la base de datos de propiedades de la CMC. Antes de activar manualmente un usuario de la CMC, verifique si existe algún usuario actual.

Si está configurando una nueva iDRAC o ha utilizado el comando racadm `racresetcfg`, el único usuario actual es el usuario `root` con la contraseña `calvin`. El subcomando `racresetcfg` restablece todos los parámetros de configuración a los valores predeterminados. Todos los cambios anteriores se pierden.

NOTA: Los usuarios se pueden activar y desactivar con el tiempo y la desactivación de un usuario no lo borra de la base de datos.

Para verificar si un usuario existe, abra una consola de texto de Telnet/SSH en la CMC, inicie sesión y escriba el siguiente comando una vez para cada índice de 1 a 16:

```
racadm getconfig -g cfgUserAdmin -i <index>
```

NOTA: También puede escribir racadm `racadm getconfig -f <myfile.cfg>` y ver o editar el archivo myfile.cfg, que incluye todos los parámetros de configuración de la CMC.

Varios parámetros e ID de objeto se muestran con sus valores actuales. Hay dos objetos importantes:

```
# cfgUserAdminIndex=XX
cfgUserAdminUserName=
```

Si el objeto `cfgUserAdminUserName` no tiene valor, el número de índice, que se indica mediante el objeto `cfgUserAdminIndex`, está disponible para usar. Si se muestra un nombre después del signo "=", ese índice lo lleva ese nombre de usuario.

Cuando se activa o desactiva manualmente un usuario con el subcomando racadm `config` , se debe especificar el índice con la opción `–i`.

El caracter "#" en los objetos de comando indica que es un objeto de solo lectura. Asimismo, si utiliza el comando racadm `racadm config -f racadm.cfg` para especificar cualquier número de grupos u objetos para escritura, el índice no se puede especificar. Un usuario nuevo se agrega al primer índice disponible. Este comportamiento permite una mayor flexibilidad a la hora de configurar una segunda CMC con los mismos valores que la CMC principal.

Adición de un usuario del CMC mediante RACADM

Para agregar un usuario nuevo a la configuración del CMC:

1 Establezca el nombre de usuario.
2 Establezca la contraseña.
3 Establezca los privilegios de usuario. Para obtener más información sobre los privilegios de usuario, consulte Tipos de usuarios.
4 Active el usuario.

Por ejemplo:

En el siguiente ejemplo se describe la forma de agregar un nuevo usuario de nombre "John" con la contraseña "123456" y privilegios de inicio de sesión en el CMC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2
john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2
123456
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege
0x00000001
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

NOTA: Para obtener una lista de valores de máscara de bits válidos para privilegios de usuario específicos, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX). El valor de privilegio predeterminado es 0, lo cual indica que los privilegios de un usuario no están activados.

Para verificar que el usuario se haya añadido correctamente con los privilegios adecuados, ejecute el siguiente comando:

```
racadm getconfig –g cfgUserAdmin –i 2
```

Para obtener más información acerca de los comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Desactivación de un usuario del CMC

Al usar RACADM, los usuarios se deben desactivar manualmente y de manera individual. Los usuarios no se pueden eliminar mediante un archivo de configuración.

Para eliminar un usuario del CMC, la sintaxis de comando es:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <index>""
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x0
```

Una cadena nula de dos caracteres de comillas ("") indica al CMC que debe eliminar la configuración de usuario en el índice especificado y restablecer los valores predeterminados originales de fábrica en la configuración de usuario.

Activación de un usuario del CMC con permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en funciones):

1 Busque un índice de usuario disponible mediante la sintaxis de comando siguiente:

```
racadm getconfig -g cfgUserAdmin -i <index>
```

2 Escriba los comandos siguientes con el nombre de usuario y la contraseñas nuevos.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <index> <user privilege bitmask value>
```

NOTA: Para obtener una lista de los valores de máscara de bits válidos para privilegios de usuario específicos, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM Chassis Management Controller for PowerEdge VRTX)* disponible en dell.com/support/manuals. El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene activado ningún privilegio.

Configuración de usuarios de Active Directory

Si la empresa utiliza el software Microsoft Active Directory, es posible configurar ese software para proporcionar acceso a la CMC, lo que permite agregar y controlar los privilegios de usuario de la CMC para los usuarios existentes en el servicio de directorio. Esta es una función con licencia.

NOTA: En los siguientes sistemas operativos, puede reconocer a los usuarios de CMC mediante Active Directory.

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

Es posible configurar la autenticación de usuario a través de Active Directory para iniciar sesión en la CMC. También puede brindar una autoridad basada en funciones, lo que permite que el administrador configure privilegios específicos para cada usuario.

Mecanismos de autentificación compatibles de Active Directory

Es posible utilizar Active Directory para definir el acceso de usuario a la CMC mediante dos métodos:

- La solución de *esquema estándar*, que solo utiliza objetos de grupo predeterminados de Active Directory de Microsoft.

- Solución de *Esquema extendido* que tiene objetos de Active Directory personalizados proporcionados por Dell. Todos los objetos de control de acceso se mantienen en Active Directory. Proporciona una flexibilidad máxima a la hora de configurar el acceso de usuario en distintas CMC con niveles de privilegios variados.

Descripción general del esquema estándar de Active Directory

Como se muestra en la figura a continuación, el uso del esquema estándar para la integración de Active Directory requiere una configuración tanto en Active Directory como en la CMC.

En Active Directory, se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso a la CMC es miembro del grupo de funciones. Para dar a este usuario acceso a una tarjeta específica de la CMC, el nombre del grupo de funciones y su nombre de dominio se deben configurar en la tarjeta específica de la CMC. La función y el nivel de privilegio se definen en cada tarjeta CMC y no en Active Directory. Puede configurar hasta cinco grupos de funciones en cada CMC. La siguiente tabla muestra los privilegios predeterminados del grupo de funciones.

Tabla 23. : Privilegios predeterminados del grupo de funciones

Grupo de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
1	Ninguno	• Usuario con acceso a la CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Administrador del servidor • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A	0x00000fff
2	Ninguno	• Usuario con acceso a la CMC • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Administrador del servidor • Usuario de alertas de prueba • Administrador de red Fabric A	0x00000ed9
3	Ninguno	Usuario con acceso a la CMC	0x00000001
4	Ninguno	Sin permisos asignados	0x00000000
5	Ninguno	Sin permisos asignados	0x00000000

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

NOTA: Para obtener más información sobre los privilegios de usuario, consulte Tipos de usuarios.

Configuración del esquema estándar de Active Directory

Para configurar la CMC para un acceso de inicio de sesión de Active Directory:

1 En un servidor de Active Directory (controladora de dominio), abra el complemento **Usuarios y equipos de Active Directory**.

2 Mediante la interfaz web de la CMC o RACADM:
   a Cree un grupo o seleccione un grupo existente.
   b Configure los privilegios de funciones.

3 Agregue el usuario de Active Directory como miembro del grupo de Active Directory para obtener acceso a la CMC.

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

NOTA: Para obtener información acerca de los distintos campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

1 En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Autentificación de usuario** > **Servicios de directorio**. Aparecerá la página **Servicios de directorio**.

2 Seleccione **Microsoft Active Directory (Esquema estándar)**. Los valores que se deben configurar para el esquema estándar se mostrarán en la misma página.

3 En la sección **Valores comunes**, especifique lo siguiente:
   - Seleccione **Activar Active Directory** e introduzca el valor de tiempo de espera para Active Directory en el campo **Tiempo de espera de AD** .
   - Para obtener las controladoras de dominio de Active Directory de una búsqueda en el DNS, seleccione **Buscar controladoras de dominio con DNS** y, a continuación, seleccione una de las opciones siguientes:
     – **Dominio de usuario desde inicio de sesión**: para realizar una búsqueda en el DNS con el nombre de dominio del usuario de inicio de sesión.
     – **Especificar un dominio**: introduzca el nombre del dominio para utilizar en la búsqueda en el DNS.
   - Para activar la CMC para utilizar las direcciones especificadas de servidores de controladoras de dominio de Active Directory, seleccione **Especificar direcciones de controladoras de dominio** . Estas direcciones de servidores son las direcciones de las controladoras de dominio en donde se ubican las cuentas de usuario y los grupos de funciones.

4 Haga clic en **Aplicar** para guardar la configuración.

   NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.

5 En la sección **Grupos de funciones del esquema estándar**, haga clic en un **Grupo de funciones**. Aparecerá la página **Configurar grupo de funciones**.

6 Especifique el nombre del grupo, el dominio y los privilegios para el grupo de funciones.

7 Haga clic en **Aplicar** para guardar la configuración del grupo de funciones y haga clic en **Volver a la página de configuración**.

8 Si ha activado la validación de certificados, debe cargar en el CMC el certificado firmado por una autoridad de certificados raíz para el bosque de dominio. En la sección **Administrar certificados**, escriba la ruta de acceso del archivo o busque el archivo de certificado. Haga clic en **Cargar** para cargar el archivo en el CMC.

   NOTA: El valor Ruta de acceso del archivo muestra la ruta de acceso relativa del archivo del certificado que está cargando. Debe escribir la ruta de acceso absoluta del archivo, que incluye la ruta de acceso completa y el nombre y la extensión del archivo completos.

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

9 Si ha activado el inicio de sesión único (SSO), en la sección **Archivo keytab de Kerberos**, haga clic en **Examinar**, especifique el archivo keytab y, a continuación, haga clic en **Cargar**. Al completarse la carga, aparecerá un mensaje que indica que la carga ha sido correcta o ha fallado.

10 Haga clic en **Aplicar**. El servidor web de la CMC se reiniciará automáticamente al hacer clic en **Aplicar**.

11 Cierre sesión y luego inicie sesión en el CMC para completar la configuración de Active Directory en el CMC.

12 Seleccione **Chasis** en el árbol del sistema y desplácese hasta la pestaña **Red**. Aparecerá la página **Configuración de red**.

13 En **Configuración de la red**, si la opción **Usar DHCP (para la dirección IP de la interfaz de red del CMC)** está seleccionada, seleccione **Usar DHCP para obtener dirección de servidor DNS**.

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

14 Haga clic en **Aplicar cambios**.

De esta forma, se completa la configuración de la función de Active Directory de esquema estándar para el CMC.

Configuración de Active Directory con esquema estándar vía RACADM

En el símbolo del sistema racadm, ejecute los comandos siguientes:

- Mediante el comando **config**:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupName <common name of the
role group>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully qualified
domain name>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege <Bit Mask
Value for specific RoleGroup permissions>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully qualified domain
name or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <fully qualified domain
name or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain
name or IP address of the domain controller>
```

NOTA: Introduzca el FQDN de la controladora de dominio, no el FQDN del dominio. Por ejemplo, introduzca `servername.dell.com` en lugar de `dell.com`.

NOTA:

Es necesario configurar al menos una de las tres direcciones. La CMC trata de conectarse con cada una de las direcciones configuradas, una a la vez, hasta establecer una conexión. Con el Esquema estándar, se trata de las direcciones de las controladoras de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog2 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog3 <fully qualified domain name
or IP address of the domain controller>
```

NOTA: El servidor de catálogo global solo 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 dominio múltiple, solamente se puede usar 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 controladora de dominio si tiene activada la validación de certificados.

Si desea desactivar la validación de certificados durante el protocolo de enlace con SSL, ejecute el siguiente comando RACADM:

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`

En este caso, no es necesario cargar el certificado de la autoridad de certificados (CA).

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`

En este caso, también debe cargar el certificado de CA con el siguiente comando de RACADM:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN del catálogo global. Asegúrese de que la DNS esté configurada correctamente.

Descripción general del esquema extendido de Active Directory

El uso del esquema extendido requiere la extensión del esquema de Active Directory.

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 los tipos de datos que se pueden agregar o incluir en la base de datos. Un ejemplo de una clase que se almacena en la base de datos es la clase usuario. Algunos ejemplos de atributos de clase de usuario son el nombre, el apellido, el número de teléfono y otros datos del usuario.

Puede ampliar la base de datos de Active Directory añadiendo sus propios *atributos* y *clases* exclusivos para requisitos específicos. Dell ha extendido el esquema para incluir los cambios necesarios y admitir la autorización y la autentificación de la administración remota mediante Active Directory.

Cada *atributo* o *clase* que se agrega a un esquema existente de Active Directory debe definirse con una identificación única. Para mantener las ID únicas en todo el sector, Microsoft mantiene una base de datos de identificadores de objetos de Active Directory (OID) para que cuando las empresas agreguen extensiones al esquema, puedan tener la garantía de que serán únicos y no entrarán en conflicto entre sí. Para extender el esquema en Microsoft Active Directory, Dell recibió OID únicos, extensiones de nombre únicas e ID de atributos con vínculos únicos para los atributos y las clases que se agregan al servicio de directorio.

- Extensión de Dell: `dell`
- OID de base de Dell: `1.2.840.113556.1.8000.1280`
- Rango de LinkID del RAC: `12070 a 12079`

Descripción general sobre las extensiones de esquema

Dell ha extendido el esquema para incluir una propiedad *Asociación*, *Dispositivo* y *Privilegio*. La propiedad *Asociación* se utiliza para vincular a los usuarios o grupos con un conjunto específico de privilegios para uno o varios dispositivos de RAC. Este modelo proporciona a un administrador la flexibilidad máxima sobre las distintas combinaciones de usuarios, privilegios de RAC y dispositivos de RAC en la red sin demasiada complexidad.

Si existen dos CMC en la red que desea integrar a Active Directory para fines de autentificación y autorización, es necesario crear al menos un objeto de asociación y un objeto de dispositivo de RAC para cada CMC. Es posible crear varios objetos de asociación y cada objeto de asociación puede ser vinculado a cuantos usuarios, grupos de usuarios u objetos de dispositivo de RAC sea necesario. Los usuarios y objetos de dispositivo de RAC pueden ser miembros de cualquier dominio en la empresa.

Sin embargo, cada objeto de asociación se puede vincular (o puede vincular usuarios, grupos de usuarios u objetos de dispositivo de RAC) a un solo objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en CMC específicas.

El objeto del dispositivo de RAC es el vínculo al firmware de RAC para consultar a Active Directory con fines de autenticación y autorización. Cuando se agrega un RAC a la red, el administrador debe configurar el RAC y su objeto de dispositivo con su nombre de

Active Directory, de modo que los usuarios puedan realizar la autenticación y la autorización con Active Directory. Además, el administrador debe agregar el RAC a por lo menos un objeto de asociación para que los usuarios puedan autenticar.

NOTA: El objeto de privilegio de RAC se aplica al CMC.

Es posible crear el número de objetos de asociación que sea necesario. Sin embargo, se debe crear al menos un objeto de asociación y se debe tener un objeto de dispositivo de RAC para cada RAC (CMC) en la red que se desee integrar con Active Directory.

El objeto de asociación permite tener tantos usuarios o grupos como sea necesario, así como objetos de dispositivo de RAC. No obstante, el objeto de asociación solo incluye un único objeto de privilegio por objeto de asociación. El objeto de asociación conecta a los *usuarios* que tienen *Privilegios* en los RAC (CMC).

Además, se pueden configurar objetos de Active Directory en un solo dominio o en varios. Por ejemplo, es posible tener dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory existentes (usuario1, usuario2 y usuario3). El usuario puede desear otorgar al usuario1 y al usuario2 un privilegio de administrador para ambas CMC, y al usuario3 un privilegio de inicio de sesión a la tarjeta de RAC2.

Al agregar Grupos universales desde dominios independientes, cree un Objeto de asociación con Ámbito universal. Los objetos de Asociación predeterminados que crea la Utilidad Dell Schema Extender son Grupos locales de dominios y no funcionan con Grupos universales de otros dominios.

Para configurar los objetos en un escenario de un solo dominio:

1 Cree dos objetos de asociación.
2 Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representen a los dos CMC.
3 Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tenga todos los privilegios (de administrador) y Priv2 tenga el privilegio de inicio de sesión.
4 Agrupe usuario1 y usuario2 en grupo1.
5 Agregue Group1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objeto de privilegio en A01, y RAC1 y RAC2 como dispositivos de RAC en A01.
6 Agregue User3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objeto de privilegio en A02, y RAC2 como dispositivo de RAC en A02.

Para configurar los objetos en un escenario de varios dominios:

1 Asegúrese de que la función de bosque del dominio esté en el modo Nativo o Windows 2003.
2 Cree dos objetos de asociación, A01 (con ámbito universal) y A02, en cualquier dominio. En la figura Configuración de objetos de Active Directory en varios dominios se muestran los objetos en Dominio2.
3 Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representen a los dos CMC.
4 Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tenga todos los privilegios (de administrador) y Priv2 tenga el privilegio de inicio de sesión.
5 Agrupe usuario1 y usuario2 en grupo1. El ámbito de grupo del Grupo1 debe ser Universal.
6 Agregue Group1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objeto de privilegio en A01, y RAC1 y RAC2 como dispositivos de RAC en A01.
7 Agregue User3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objeto de privilegio en A02, y RAC2 como dispositivo de RAC en A02.

Configuración del esquema extendido de Active Directory

Para configurar Active Directory para obtener acceso a la CMC:

1 Amplíe el esquema de Active Directory.
2 Amplíe el complemento Usuarios y equipos de Active Directory.
3 Agregue usuarios de la CMC y sus privilegios en Active Directory.
4 Active SSL en cada una de las controladoras de dominio.
5 Configure las propiedades de Active Directory para la CMC mediante la interfaz web de la CMC o de RACADM.

Extensión del esquema de Active Directory

Al extender el esquema de Active Directory se agrega una unidad organizacional de Dell, clases y atributos de esquema y ejemplos de privilegios y objetos de asociación al esquema de Active Directory. Antes de extender el esquema, asegúrese de tener privilegios de Administrador de esquema en el propietario del rol de operaciones de maestro único flexible (FSMO) de maestro de 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 (Herramientas y documentación de Dell Systems Management)*, en los siguientes directorios respectivos:

- Unidad de DVD:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools\Remote_Management_Advanced\Schema Extender

Para usar los archivos LDIF, consulte las instrucciones en las notas de publicación que se incluyen en el directorio **LDIF_Files**.

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 asegurarse de que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la **Welcome (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 **Finalizar**.

   El esquema ha sido extendido. Para verificar la extensión del esquema, utilice el complemento de esquema de Active Directory y el MMC para verificar que las clases y los atributos existan. Para obtener más información sobre las clases y los atributos, consulte Clases y atributos. Consulte la documentación de Microsoft para obtener detalles acerca del uso de MMC y el complemento de esquema de Active Directory.

Clases y atributos

Tabla 24. Definiciones de clases para 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 25. Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo Dell RAC RAC debe configurarse como delliDRACDevice en Active Directory. Esta configuración permite que CMC envíe solicitudes de Protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 26. Clase delliDRACAssociationObject

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Descripción	Representa el objeto de asociación de Dell. Este proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Grupo
Atributos	dellProductMembers dellPrivilegeMember

Tabla 27. Clase dellRAC4Privileges

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

Tabla 28. 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

OID	1.2.840.113556.1.8000.1280.1.1.1.4
SuperClasses	Usuario
Atributos	dellRAC4Privileges

Tabla 29. Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	dellAssociationMembers

Tabla 30. Lista de atributos agregados al esquema de Active Directory

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Atributo: `dellPrivilegeMember` **Descripción**: lista de objetos `dellPrivilege` que pertenecen a este atributo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.1 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellProductMembers` **Descripción**: lista de objetos `dellRacDevices` que pertenecen a esta función. Este atributo es el vínculo de avance para el vínculo de retroceso `dellAssociationMembers`. **Identificación de vínculo**: 12070 **OID**: 1.2.840.113556.1.8000.1280.1.1.2.2 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellIsCardConfigAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de configuración de tarjeta en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsLoginUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de inicio de sesión en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsUserConfigAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de configuración de usuario en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.5	VERDADERO

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Atributo: `dellIsLogClearAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de borrado de registros en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsServerResetUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos para restablecer el servidor en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsTestAlertUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de usuario de alertas de prueba en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsDebugCommandAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de comandos de depuración en el dispositivo. **OID**: 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)	VERDADERO
Atributo: `dellSchemaVersion` **Descripción**: se utiliza la versión de esquema actual para actualizar el esquema. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.12 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
Atributo: `dellRacType` **Descripción**: este atributo representa el tipo de RAC actual para el objeto dellRacDevice y el vínculo de retroceso al vínculo de avance dellAssociationObjectMembers. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.13 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
Atributo: `dellAssociationMembers` **Descripción:** Lista de los objetos dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso para el atributo vinculado dellProductMembers. **Identificación de vínculo**: 12071 **OID:** 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)	FALSO

OID asignado/Identificador de objeto de sintaxis	Con un solo valor

Atributo: `dellPermissionsMask1`

OID: 1.2.840.113556.1.8000.1280.1.6.2.1 número entero (LDAPTYPE_INTEGER)

Atributo: `dellPermissionsMask2`

OID: 1.2.840.113556.1.8000.1280.1.6.2.2 número entero (LDAPTYPE_INTEGER)

Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory

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

Cuando instale el Systems Management Software con el DVD de *herramientas y documentación de Dell Systems Management* puede instalar el complemento si selecciona la opción **Complemento de usuarios y equipos de Active Directory**. Consulte la *Guía de instalación rápida del software Dell OpenManage* para obtener instrucciones adicionales sobre la instalación de software de administración de sistemas. Para sistemas operativos Windows de 64 bits, el instalador del complemento se ubica en **< Unidad de DVD>:\SYSMGMT \ManagementStation\support\ ory_SnapIn64.**

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

Agregar usuarios y privilegios del CMC a Active Directory

Mediante el complemento Usuarios y equipos de Active Directory extendido de Dell, es posible agregar usuarios y privilegios de la CMC al crear objetos de dispositivo de RAC, de asociación y de privilegio. Para agregar cada objeto, realice los pasos siguientes:

- Cree un objeto de dispositivo de RAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Creación de un objeto de dispositivo de RAC

Para crear un objeto de dispositivo de RAC:

1. En la ventana **Raíz de consola de MMC**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.
3. En la página **Nuevo objeto**, escriba un nombre para el objeto nuevo. El nombre debe ser idéntico al nombre de la CMC que se introduce en la Configuración de Active Directory con el esquema estándar mediante la interfaz web.
4. Seleccione **Objeto de dispositivo de RAC** y haga clic en **Aceptar**.

Creación de un objeto de privilegio

Para crear un objeto de privilegio:

NOTA: Debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola de MMC**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.
3. En la página **Nuevo objeto**, escriba un nombre para el objeto nuevo.

4 Seleccione **Objeto de privilegio** y haga clic en **Aceptar**.

5 Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.

6 Haga clic en la ficha **Privilegios de RAC** y asigne los privilegios para el usuario o grupo. Para obtener más información sobre los privilegios de usuario del CMC, consulte Tipos de usuarios.

Creación de un objeto de asociación

El objeto de asociación se deriva de un grupo y debe contener un tipo de grupo. El alcance de la asociación especifica el tipo de grupo de seguridad para el objeto de asociación. Al crear un objeto de asociación, elija el alcance de la asociación correspondiente al tipo de objetos que quiere agregar. Por ejemplo, si selecciona Universal los objetos de asociación solo estarán disponibles cuando el dominio de Active Directory funcione en el modo nativo o superior.

Para crear un objeto de asociación:

1 En la ventana **Raíz de consola (MMC)**, haga clic con el botón derecho del mouse en un contenedor.

2 Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.

3 En la página **Nuevo objeto**, escriba un nombre para el objeto nuevo y seleccione **Objeto de asociación**.

4 Seleccione el ámbito para **Objeto de asociación** y haga clic en **Aceptar**.

Adición de 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 RAC o grupos de dispositivos RAC. Si el sistema se ejecuta con el sistema operativo Microsoft Windows 2000 o una versión posterior, use grupos universales para abarcar dominios con el usuario o los objetos de RAC.

Es posible agregar grupos de usuarios y dispositivos de RAC.

Adición de usuarios o grupos de usuarios

Para agregar usuarios o grupos de usuarios:

1 Haga clic con el botón derecho del mouse en **Objeto de asociación** y seleccione **Propiedades**.

2 Seleccione la ficha **Usuarios** y haga clic en **Agregar**.

3 Introduzca el nombre del grupo de usuarios o del usuario y haga clic en **Aceptar**.

Adición de privilegios

Para agregar privilegios:

1 Seleccione la ficha **Objetos de privilegios** y haga clic en **Agregar**.

2 Introduzca 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 al autentificar un dispositivo RAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

Forma de agregar dispositivos de RAC o grupos de dispositivos de RAC

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

1 Seleccione la ficha **Productos** y haga clic en **Agregar**.

2 Introduzca el nombre de los dispositivos de RAC o de los grupos de dispositivos de RAC y haga clic en **Aceptar**.

3 En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

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

Configuración de Active Directory con esquema extendido mediante la interfaz web del CMC

Para configurar Active Directory con esquema extendido mediante la interfaz web del CMC:

NOTA: Para obtener información acerca de los distintos campos, consulte la *Online Help*.

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Autenticación del usuario** > **Descripción general del chasis** > **Servicios Directory**.

2 Seleccione **Microsoft Active Directory (esquema extendido)**.

Las opciones a configurar para el esquema extendido aparecerán en la misma página.

3 En la sección **Valores comunes**, especifique lo siguiente:

- Seleccione **Activar Active Directory** e introduzca el valor de tiempo de espera para Active Directory en el campo **Tiempo de espera de AD** .
- Para obtener las controladoras de dominio de Active Directory de una búsqueda en el DNS, seleccione **Buscar controladoras de dominio con DNS** y, a continuación, seleccione una de las opciones siguientes:
  - **Dominio de usuario desde inicio de sesión**: para realizar una búsqueda en el DNS con el nombre de dominio del usuario de inicio de sesión.
  - **Especificar un dominio**: introduzca el nombre del dominio para utilizar en la búsqueda en el DNS.
- Para activar la CMC para utilizar las direcciones especificadas de servidores de controladoras de dominio de Active Directory, seleccione **Especificar direcciones de controladoras de dominio** . Estas son las direcciones de las controladoras de dominio donde se encuentran el objeto dispositivo de la CMC y los objetos de asociación.

4 Haga clic en **Aplicar** para guardar la configuración.

NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.

5 En la sección **Configuración del esquema extendido**, escriba el nombre del dispositivo de CMC y el nombre de dominio.

6 Si ha activado la validación de certificados, debe cargar en el CMC el certificado firmado por una autoridad de certificados raíz para el bosque de dominio. En la sección **Administrar certificados**, escriba la ruta de acceso del archivo o busque el archivo de certificado. Haga clic en **Cargar** para cargar el archivo en el CMC.

NOTA: El valor `File Path` muestra la ruta de acceso relativa del archivo del certificado que está cargando. Debe escribir la ruta de acceso absoluta del archivo, que incluye la ruta de acceso completa y el nombre y la extensión del archivo completos.

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

PRECAUCIÓN: La validación de certificados SSL se requiere de forma predeterminada. No se recomienda desactivar este certificado.

7 Si ha activado el inicio de sesión único (SSO), en la sección Archivo keytab de Kerberos, haga clic en **Examinar**, especifique el archivo keytab y, a continuación, haga clic en **Cargar**. Al completarse la carga, aparecerá un mensaje que indica que la carga ha sido correcta o ha fallado.

8 Haga clic en **Aplicar**.

El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.

9 Inicie sesión en la interfaz web del CMC.

10 En el árbol del sistema, seleccione **Chasis**, haga clic en la pestaña **Red** y luego en la subpestaña **Red**. Aparecerá la página **Configuración de red**.

11 Si la opción **Usar DHCP** para la dirección IP de la interfaz de red del CMC está activada, realice una de las siguientes operaciones:

- Seleccione la opción **Usar DHCP para obtener direcciones de servidor DNS** a fin de permitir que el servidor DHCP obtenga las direcciones del servidor DNS automáticamente.

- Configure manualmente una dirección IP de servidor DNS. Para eso, desactive la casilla **Usar DHCP para obtener direcciones de servidor DNS** y escriba las direcciones IP de los servidores DNS primario y alternativo en los campos correspondientes.

12 Haga clic en **Aplicar cambios**.

Se habrán configurado las opciones de Active Directory para el esquema extendido.

Configuración de Active Directory con esquema extendido mediante RACADM

Para configurar Active Directory de CMC con esquema extendido mediante los comandos RACADM, abra el símbolo del sistema e introduzca los siguientes comandos en el símbolo del sistema:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacName <RAC common name>
racadm config -g cfgActiveDirectory -o cfgADRacDomain < fully qualified rac domain name >
racadm config -g cfgActiveDirectory -o cfgADDomainController1 < fully qualified domain name or
IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController2 < fully qualified domain name or
IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController3 < fully qualified domain name or
IP Address of the domain controller >
```

NOTA: Debe configurar al menos una de las tres direcciones. La CMC trata de conectarse con cada una de las direcciones configuradas, una a la vez, hasta establecer una conexión. Con el esquema extendido, estas son las direcciones FQDN o IP de las controladoras de dominio donde se encuentra este dispositivo de la CMC.

Para desactivar la validación de certificado durante el protocolo de enlace (opcional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

NOTA: En este caso, no tiene que cargar un certificado de CA.

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

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

En este caso, debe cargar un certificado de CA.

```
racadm sslcertupload -t 0x2 -f < ADS root CA certificate >
```

NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN. Asegúrese de que la DNS esté configurada correctamente.

El siguiente comando de RACADM es opcional:

```
racadm sslcertdownload -t 0x1 -f < RAC SSL certificate >
```

Configuración de los usuarios LDAP genéricos

La CMC proporciona una solución genérica para admitir la autentificación basada en el Protocolo ligero de acceso a directorios (LDAP). Esta función no requiere ninguna extensión del esquema en los servicios de directorio.

Ahora, un administrador de la CMC puede integrar los inicios de sesión de los usuarios del servidor LDAP con la CMC. Esta integración requiere una configuración en el servidor LDAP y en la CMC. En el servidor LDAP, se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso a la CMC se convierte en miembro del grupo de funciones. Los privilegios se continúan almacenando en la CMC para la autorización, de forma similar a la configuración de esquema estándar compatible con Active Directory.

Para activar el usuario LDAP de modo que tenga acceso a una tarjeta específica de la CMC, el nombre del grupo de funciones y su nombre de dominio se deben configurar en la tarjeta específica de la CMC. Puede configurar un máximo de cinco grupos de funciones en cada CMC. Existe la opción de agregar un usuario a varios grupos dentro del servicio de directorio. Si un usuario es miembro de varios grupos, obtiene los privilegios de todos sus grupos.

Para obtener información sobre el nivel de privilegios de los grupos de funciones y los valores predeterminados de esos grupos, consulte Tipos de usuarios.

Configuración del directorio LDAP genérico para acceder a CMC

La implementación de LDAP genérico del CMC utiliza dos fases para otorgar acceso a la autentificación usuario-usuario y a la autorización de usuarios.

Autentificación de usuarios LDAP

Algunos servidores de directorio requieren un enlace antes de que pueda buscarse un servidor LDAP específico.

Para autentificar un usuario:

1 De forma opcional, establezca un vínculo con el servicio de directorio. La opción predeterminada es un vínculo anónimo.

NOTA: Los servidores del directorio basado en Windows no permiten un inicio de sesión anónimo. Por lo tanto, introduzca el nombre y la contraseña de DN del vínculo.

2 Busque el usuario según el nombre de inicio de sesión del mismo. El atributo predeterminado es `uid`. Si se encuentra más de un objeto, el proceso arroja un mensaje de error.

3 Anule el enlace y establezca un enlace con el DN y la contraseña de usuario. Si el sistema no se puede vincular, el inicio de sesión no será posible.

4 Si estos pasos se completan correctamente, el usuario se considera autentificado.

Autorización de usuarios LDAP

Para autorizar un usuario:

1 Buscar en cada grupo configurado el nombre de dominio del usuario en los atributos `member or uniqueMember`. Un administrador puede configurar el dominio de un usuario.

2 Otórguele al usuario derechos y privilegios de acceso adecuados para cada grupo de usuarios al que este pertenece.

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web del CMC

Para configurar el servicio de directorio LDAP genérico:

NOTA: Es necesario contar con el privilegio de Administrador de configuración del chasis.

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Autentificación de usuario** > **Servicios de directorio**.

2 Seleccione **LDAP genérico**.

Los valores que se deben configurar para el esquema estándar se mostrarán en la misma página.

3 Especifique lo siguiente:

NOTA: Para obtener información acerca de los distintos campos, consulte la *Online Help*.

- Configuración común
- Servidor que se debe usar con LDAP:
  - Servidor estático: especifique la dirección IP o el nombre de dominio completo y el número de puerto LDAP.

– Servidor DNS: especifique el servidor DNS para recuperar una lista de los servidores LDAP. Para eso, busque el registro de SRV dentro de DNS.

  Se ejecutará la siguiente consulta de DNS para los registros de SRV:

  ```
  _[Service Name]._tcp.[Search Domain]
  ```

  donde *Search Domain* es el dominio de nivel raíz que se utiliza en la consulta y *Service Name* indica el nombre del servicio que se debe utilizar en la consulta.

  Por ejemplo:

  ```
  _ldap._tcp.dell.com
  ```

  donde `ldap` es el nombre del servicio y `dell.com` es el dominio de búsqueda.

4 Haga clic en **Aplicar** para guardar la configuración.

NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.

5 En la sección **Configuración de grupo**, haga clic en un **Grupo de funciones**.

6 En la página **Configurar grupo de funciones de LDAP**, especifique los privilegios y el nombre del dominio del grupo para el grupo de funciones.

7 Haga clic en **Aplicar** para guardar la configuración del grupo de funciones, haga clic en **Volver a la página de configuración** y seleccione **LDAP genérico**.

8 Si ha seleccionado la opción **Validación de certificados activada**, en la sección **Administrar certificados** debe especificar el certificado de CA para validar el certificado del servidor LDAP durante el protocolo de enlace SSL y hacer clic en **Cargar**. El certificado se cargará en el CMC y aparecerán los detalles.

9 Haga clic en **Aplicar**.

Se habrá configurado el servicio de directorio LDAP.

Configuración del servicio de directorio LDAP genérico mediante RACADM

Para configurar el servicio de directorio LDAP, utilice los objetos en los grupos RACADM `cfgLdap` y `cfgLdapRoleGroup`.

Existen muchas opciones para configurar los inicios de sesión de LDAP. En la mayoría de los casos, algunas opciones pueden utilizarse con su configuración predeterminada.

NOTA: Se recomienda seriamente utilizar el comando racadm `testfeature -f LDAP` para probar la configuración inicial de LDAP. Esta función admite IPv4 e IPv6.

Los cambios de propiedades necesarios incluyen la activación de inicios de sesión de LDAP, la definición de un nombre de dominio completo o una dirección IP para el servidor y la configuración del DN de base del servidor LDAP.

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=
  company,dc=com
  ```

La CMC puede configurarse para realizar una consulta opcional en el servidor DNS para solicitar registros de SRV. Si la propiedad `cfgLDAPSRVLookupEnable` está activada, la propiedad `cfgLDAPServer` se ignora. La siguiente consulta se utiliza para buscar registros de SRV en el DNS:

```
_ldap._tcp.domainname.com
```

En esta consulta, `ldap` es la propiedad `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` se configura para ser **domainname.com**.
```

Para obtener más información acerca de los comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support/manuals**.

10

Configuración del CMC para inicio de sesión único o inicio de sesión mediante tarjeta inteligente

En esta sección se proporciona información para configurar la CMC para el inicio de sesión único (SSO) y el inicio de sesión mediante tarjeta inteligente en los usuarios de Active Directory.

El inicio de sesión único utiliza Kerberos como método de autenticación, lo que permite que los usuarios que han realizado un inicio de sesión único o automático tengan acceso a las aplicaciones subsiguientes como Exchange. Para el inicio de sesión único, la CMC utiliza las credenciales del sistema cliente que el sistema operativo almacena en caché después de que el usuario inicia sesión mediante una cuenta de Active Directory válida.

La autentificación de dos factores proporciona un mayor nivel de seguridad, ya que requiere que los usuarios dispongan de una contraseña o PIN y una tarjeta física con una clave privada o un certificado digital. Kerberos usa este mecanismo de autentificación de dos factores, con el que los sistemas pueden probar su autenticidad.

NOTA: Cuando se selecciona un método de inicio de sesión, no se determinan los atributos de política relacionados con otras interfaces de inicio de sesión, por ejemplo, SSH. También se deben establecer otros atributos de política para las demás interfaces de inicio de sesión. Si desea desactivar todas las demás interfaces de inicio de sesión, vaya a la página Servicios y desactive todas las interfaces de inicio de sesión (o algunas).

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 y Windows Server 2008 pueden usar Kerberos como el mecanismo de autentificación para el inicio de sesión único y el inicio de sesión mediante tarjeta inteligente.

Para obtener información sobre Kerberos, consulte el sitio web de Microsoft.

Temas:

Requisitos del sistema

Para utilizar la autentificación de Kerberos, la red debe incluir:

- Servidor DNS
- Servidor de Microsoft Active Directory

NOTA: Si usa Active Directory en Microsoft Windows 2003, asegúrese de tener las revisiones y los Service Packs más recientes instalados en el sistema cliente. Si usa Active Directory en Microsoft Windows 2008, asegúrese de tener instalado SP1 junto con los siguientes hotfixes:

Windows6.0-KB951191-x86.msu para la utilidad KTPASS. Sin esta revisión, la utilidad genera archivos keytab dañados.

Windows6.0-KB957072-x86.msu para utilizar transacciones GSS_API y SSL durante un enlace de LDAP.

- Centro de distribución de claves Kerberos (se incluye con el software de servidor Active Directory).
- Servidor DHCP (recomendado).
- La zona inversa del servidor DNS debe tener una entrada para el servidor Active Directory y la CMC.

Sistemas cliente

- Solamente para el inicio de sesión mediante tarjeta inteligente, el sistema cliente debe tener el paquete redistribuible Microsoft Visual C++ 2005. Para obtener más información, consulte **www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- Para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente, el sistema cliente debe formar parte del dominio de Active Directory y del territorio de Kerberos.

CMC

- Cada CMC debe tener una cuenta de Active Directory.
- El CMC debe formar parte del dominio de Active Directory y del territorio de Kerberos.

Prerrequisitos para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente

A continuación se indican los prerrequisitos para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente:

- Configure el territorio de Kerberos y el centro de distribución de claves (KDC) para Active Directory (ksetup).
- Una sólida infraestructura de NTP y DNS para evitar problemas de desfase de tiempo y búsqueda inversa.
- Configure la CMC y el grupo de funciones de esquema estándar de Active Directory con miembros autorizados.
- Para la tarjeta inteligente, cree usuarios de Active Directory para cada CMC, configurados para utilizar el cifrado DES de Kerberos pero no la preautentificación.
- Configure el explorador para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente.
- Registre a los usuarios de CMC en el centro de distribución de claves con Ktpass (esto también genera una clave que se carga en la CMC).

Generación del archivo Keytab de Kerberos

Para admitir la autentificación de inicio de sesión único (SSO) y de inicio de sesión mediante tarjeta inteligente, la CMC admite la red Kerberos de Windows. La herramienta ktpass (disponible en Microsoft como parte del CD/DVD de instalación de servidores) se utiliza para crear enlaces de nombre principal de servicio (SPN) a una cuenta de usuario y exportar la información de confianza a un archivo keytab de Kerberos de estilo MIT. Para obtener más información sobre la utilidad ktpass, consulte el sitio web de Microsoft.

Antes de generar un archivo keytab, debe crear una cuenta de usuario de Active Directory para usar con la opción **-mapuser** del comando ktpass. Debe usar el mismo nombre que el nombre DNS de la CMC al que desea cargar el archivo keytab generado.

Para generar un archivo keytab mediante la herramienta ktpass:

1 Ejecute la utilidad *ktpass* en la controladora de dominio (servidor de Active Directory) donde desee asignar el CMC a una cuenta de usuario en Active Directory.

2 Utilice el comando `ktpass` siguiente para crear el archivo keytab de Kerberos:

```
ktpass -princ HTTP/cmcname.domainname.com@DOMAINNAME.COM -mapuser keytabuser -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

NOTA: `cmcname.domainname.com` debe estar en minúsculas como exige RFC y `@REALM_NAME` debe estar en mayúsculas. Además, la CMC admite los tipos de criptografía DES-CBC-MD5 y AES256-SHA1 para la autenticación de Kerberos.

Se generará un archivo keytab que se debe cargar en el CMC.

NOTA: El archivo keytab contiene una clave de cifrado y debe conservarse en un lugar seguro. Para obtener más información sobre la utilidad *ktpass*, consulte el sitio web de Microsoft.

Configuración del CMC para el esquema de Active Directory

Para obtener información sobre la forma de configurar la CMC para el esquema estándar de Active Directory, consulte Configuración del esquema estándar de Active Directory.

Para obtener información sobre la forma de configurar la CMC para el esquema extendido de Active Directory, consulte Descripción general del esquema extendido de Active Directory.

Configuración del explorador para el inicio de sesión único

El inicio de sesión único (SSO) es compatible con Internet Explorer versiones 6.0 y superiores, y Firefox versiones 3.0 y superiores.

NOTA: Las instrucciones siguientes se aplican solamente si la CMC utiliza el inicio de sesión único con la autentificación de Kerberos.

Internet Explorer

Para configurar Internet Explorer para inicio de sesión único:

1 En Internet Explorer, seleccione **Herramientas** > **Opciones de Internet**.

2 En la ficha **Seguridad**, en **Seleccione una zona para ver o cambiar la configuración de seguridad**, seleccione **Intranet local**.

3 Haga clic en **Sitios**.

Se muestra el cuadro de diálogo **Intranet local**.

4 Haga clic en **Avanzado**.

Se muestra el cuadro de diálogo **Configuración avanzada de Intranet local**.

5 En el campo **Agregar este sitio a la zona**, escriba el nombre del CMC y el dominio al cual pertenece y haga clic en **Agregar**.

NOTA: Se puede utilizar un comodín (*) para especificar todos los dispositivos o usuarios de ese dominio.

Mozilla Firefox

1 En Firefox, escriba **about:config** en la barra de direcciones.

NOTA: Si el explorador muestra la advertencia Esto puede anular su garantía, haga clic en Seré cuidadoso. Lo prometo.

2 En el cuadro de texto **Filtro**, escriba **negotiate**.

El explorador muestra una lista de nombres preferidos limitada a aquéllos que contienen la palabra "negotiate".

3 En la lista, haga doble clic en **network.negotiate-auth.trusted-uris**.

4 En el cuadro de diálogo **Ingresar valor de la cadena**, escriba el nombre de dominio del CMC y haga clic en **Aceptar**.

Configuración de un explorador para el inicio de sesión mediante tarjeta inteligente

Internet Explorer: asegúrese de que el explorador de Internet esté configurado para descargar los complementos Active-X.

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory

Es posible usar la interfaz web del CMC o RACADM para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente en el CMC.

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory mediante la interfaz web

Para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente de Active Directory en el CMC:

NOTA: Para obtener más información acerca de estas opciones, consulte *Online Help*.

1 Mientras configura Active Directory, para establecer una cuenta de usuario, realice los siguientes pasos adicionales:

- Cargue el archivo keytab.
- Para activar el inicio de sesión único, seleccione la opción **Activar inicio de sesión único**.
- Para activar el inicio de sesión mediante tarjeta inteligente, seleccione la opción **Activar inicio de sesión mediante tarjeta inteligente**.

NOTA: Si estas dos opciones están seleccionadas, todas las interfaces fuera de banda de línea de comandos, incluida secure shell (SSH), Telnet, serie y RACADM remoto permanecen sin cambios.

2 Haga clic en **Aplicar**.

La configuración se guarda.

Es posible probar Active Directory con la autentificación de Kerberos mediante el comando de RACADM:

```
testfeature -f adkrb -u <user>@<domain>
```

donde <*user*> es una cuenta de usuario de Active Directory válida.

Una ejecución satisfactoria de este comando indica que la CMC puede adquirir las credenciales Kerberos y obtener acceso a la cuenta de Active Directory del usuario. Si el comando no se ejecuta satisfactoriamente, resuelva el error y vuelva a ejecutar el comando. Para obtener más información, consulte la *Guía de referencia sobre la línea de comando RACADM de Chassis Management Controller para PowerEdge VRTX* que está disponible en dell.com/support/manuals.

Carga de un archivo keytab

El archivo keytab de Kerberos sirve como credencial de nombre de usuario y contraseña de la CMC para el centro de datos de Kerberos (KDC), que a su vez autoriza el acceso a Active Directory. Cada CMC dentro del dominio de Kerberos se debe registrar con Active Directory y debe tener un archivo keytab exclusivo.

Puede cargar un archivo keytab de Kerberos generado en el servidor de Active Directory asociado. Se puede generar el archivo keytab de Kerberos desde el servidor de Active Directory ejecutando la utilidad **ktpass.exe**. Este archivo keytab establece una relación de confianza entre el servidor de Active Directory y la CMC.

Para cargar el archivo keytab:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Autentificación de usuario** > **Servicios de directorio**.
2 Seleccione **Microsoft Active Directory (Esquema estándar)**.
3 En la sección **Archivo keytab de Kerberos**, haga clic en **Examinar**, seleccione el archivo keytab y haga clic en **Cargar**.
Una vez completada la carga, se mostrará un mensaje donde se indicará si el archivo keytab se ha cargado correctamente o no.

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory mediante RACADM

Además de los pasos que se realizan durante la configuración de Active Directory, ejecute el siguiente comando para activar el inicio de sesión único:

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

Además de los pasos que se realizan durante la configuración de Active Directory, utilice los siguientes objetos para activar el inicio de sesión mediante tarjeta inteligente:

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

Configuración del CMC para el uso de consolas de línea de comandos

En esta sección se proporciona información acerca de las funciones de la consola de línea de comandos (o la consola de conexión de serie/Telnet/Secure Shell) de la CMC y se indica cómo configurar el sistema para poder ejecutar acciones de administración de sistemas a través de la consola. Para obtener información sobre el uso de los comandos RACADM en la CMC a través de la consola de línea de comandos, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Temas:

Funciones de la consola de línea de comandos del CMC

La CMC admite las siguientes funciones de consola serie, Telnet y SSH:

- Una conexión de cliente serie y hasta cuatro conexiones simultáneas de cliente Telnet.
- Hasta cuatro conexiones simultáneas de cliente Secure Shell (SSH).
- Compatibilidad para comandos RACADM.
- Comando de conexión integrado que se conecta a la consola serie de servidores y a los módulos de E/S; también disponible como `racadm connect`.
- Historial y edición de línea de comandos.
- Control del tiempo de espera de las sesiones en todas las interfaces de consola.

Comandos para la interfaz de la línea de comandos del CMC

Al conectarse a la línea de comandos de la CMC, puede ingresar estos comandos:

Tabla 31. Comandos para la línea de comandos del CMC

Comando	Descripción
`racadm`	Los comandos RACADM comienzan con la palabra clave `racadm`), seguida de un subcomando. Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la*

Comando	Descripción
	línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).
`connect`	Se conecta a la consola de serie de un servidor o módulo de E/S. Para obtener más información, consulte Conexión a servidores o módulos de E/S con el comando connect. **NOTA: También se puede usar el comando RACADM `connect`.**
`exit`, `logout`, y `quit`	Todos estos comandos ejecutan la misma acción. Terminan la sesión actual y regresan a una interfaz de línea de comandos de inicio de sesión.

Uso de una consola Telnet con el CMC

Es posible mantener hasta cuatro sesiones Telnet con la CMC de forma simultánea.

Si su estación de administración ejecuta Microsoft Windows XP o Microsoft Windows Server 2003, es posible que tenga un problema con los caracteres en la sesión Telnet de la CMC. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión en el que la tecla de retorno no responde y no aparece la petición de contraseña.

Para solucionar este problema, descargue el hotfix 824810 en **support.microsoft.com**. Para obtener más información, también puede consultar el artículo 824810 de Microsoft Knowledge Base.

En la interfaz de la línea de comandos, puede administrar los tiempos de espera de las sesiones a través del comando racadm, `racadm getconfig -g cfgSessionManagement`. Para obtener más información, consulte la *Chassis Management Controller Version for Dell PowerEdge VRTX Command Line Reference Guide* (Guía de referencia de la versión de Chassis Management Controller para la línea de comandos de Dell PowerEdge VRTX).

Uso de SSH con el CMC

SSH es una sesión de línea de comandos que incluye las mismas funciones que una sesión Telnet, pero con negociación de sesiones y cifrado para mejorar la seguridad. La CMC admite la versión 2 de SSH con autentificación de contraseña. SSH está activado en la CMC de manera predeterminada.

NOTA: La CMC no admite la versión 1 de SSH.

Cuando se presenta un error durante el inicio de sesión en la CMC, el cliente SSH envía un mensaje de error. El texto del mensaje depende del cliente y el CMC no lo controla. Revise los mensajes de RACLog para determinar la causa de la falla.

NOTA: `OpenSSH` se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. También puede ejecutar `OpenSSH` mediante Putty.exe. La ejecución de `OpenSSH` en el símbolo del sistema de Windows no proporciona una funcionalidad completa, es decir, algunas teclas no responderán y no se mostrarán gráficos. En servidores que ejecutan Linux, ejecute los servicios del cliente SSH para conectarse a la CMC con cualquier shell.

Se admiten cuatro sesiones simultáneas de SSH a la vez. El tiempo de espera de la sesión está controlado por la propiedad. `cfgSsnMgtSshIdleTimeout` Puede comprobar los diversos tiempos de espera de la sesión mediante el comando racadm, `getconfig -g cfgSessionManagement`.

```
$ racadm getconfig -g cfgSessionManagement
cfgSsnMgtWebserverTimeout=1800
cfgSsnMgtTelnetIdleTimeout=1800
cfgSsnMgtSshIdleTimeout=1800
cfgSsnMgtRacadmTimeout=60
```

Para obtener más información acerca de los comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en dell.com/support/manuals.

La CMC también admite la Autentificación de clave pública (PKA) en SSH. Este método de autentificación mejora la automatización de las secuencias de comandos de SSH al evitar la necesidad de incorporar o solicitar la ID/contraseña del usuario. Para obtener más información, consulte Configuración de la autentificación de clave pública en SSH.

SSH está activada de manera predeterminada. Cuando la opción SSH está desactivada, es posible activarla por medio de cualquier otra interfaz admitida.

Para configurar SSH, consulte Configuring Services (Configuración de servicios).

Esquemas de criptografía SSH compatibles

Para comunicarse con la CMC mediante el protocolo SSH, se admiten varios esquemas de criptografía que se enumeran en la tabla siguiente.

Tabla 32. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS de 512–1024 bits (aleatorio) 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 del mensaje	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Autentificación	Contraseña

Configuración de la autentificación de clave pública en SSH

Puede configurar hasta seis claves públicas que se pueden utilizar con el nombre de usuario de servicio a través de la interfaz de SSH. Antes de agregar o eliminar claves públicas, asegúrese de utilizar el comando `view` para ver las claves que ya están configuradas y no sobrescribir ni eliminar accidentalmente una clave. El nombre de usuario del servicio es una cuenta de usuario especial que se puede utilizar para acceder a la CMC mediante SSH. Cuando la autentificación de clave pública en SSH se configura y se utiliza correctamente, no es necesario introducir un nombre de usuario o contraseña para iniciar sesión en la CMC. Esta función puede resultar de gran utilidad para configurar secuencias de comandos automáticas para ejecutar diversas funciones.

NOTA: No hay soporte de interfaz gráfica de usuario para administrar esta función; solamente se puede utilizar RACADM.

Al agregar claves públicas nuevas, asegúrese de que las claves existentes no se encuentren ya en el índice donde se agrega la clave nueva. La CMC no realiza comprobaciones para verificar que las claves anteriores se hayan eliminado antes de agregar una nueva. Tan pronto como se agrega una clave nueva, esa clave entra en vigor automáticamente mientras la interfaz de SSH esté activada.

Cuando utilice la sección de comentario de la clave pública, recuerde que la CMC solo utiliza los primeros 16 caracteres. La CMC utiliza el comentario de la clave pública para distinguir a los usuarios de SSH cuando se utiliza el comando RACADM `getssninfo` , ya que todos los usuarios de autentificación de clave pública usan el nombre de usuario de servicio para iniciar sesión.

Por ejemplo, si se configuran dos claves públicas, una con el comentario PC1 y otra con el PC2:

```
racadm getssninfo
Type       User   IP Address   Login
Date/Time
SSH        PC1    x.x.x.x      06/16/2009
09:00:00
SSH        PC2    x.x.x.x      06/16/2009
09:00:00
```

Para obtener más información sobre `sshpkauth`, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Generación de claves públicas para sistemas que ejecutan Windows

Antes de agregar una cuenta, se requiere una clave pública del sistema que obtendrá acceso a la CMC en SSH. Hay dos maneras de generar el par de claves pública-privada: mediante la aplicación Generador de claves PuTTY para clientes que ejecutan Windows o la CLI ssh-keygen para clientes que ejecutan Linux.

En esta sección se describen instrucciones sencillas para generar un par de claves pública-privada para ambas aplicaciones. Para ver usos adicionales o avanzados de estas herramientas, consulte la aplicación Ayuda.

Para usar el Generador de claves PuTTY a fin de crear una clave básica para clientes que ejecutan Windows:

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 Especifique la cantidad de bits para la clave. Asegúrese de que el tamaño de la clave de RSA sea entre 1024 y 4096.

NOTA:

- La longitud de la clave DSA recomendada es 1024.
- Es posible que el CMC no muestre un mensaje si se agregan claves menores que 1024 o mayores que 4096, pero el CMC deja de responder si se intenta iniciar sesión con esas claves.
- Para claves DSA superiores a 2048, utilice el siguiente comando RACADM. La CMC acepta las claves RSA hasta la clave 4096, pero la fortaleza recomendada de la clave es 1024.

```
racadm -r 192.168.8.14 -u root -p calvin sshpkauth -i svcacct -k 1 -p 0xfff -f
dsa_2048.pub
```

3 Haga clic en **Generar** y mueva el mouse en la ventana, tal como se indica.

Después de crear la clave, se puede modificar el campo de comentario de la clave.

También se puede especificar una frase de contraseña para proteger la clave. Asegúrese de guardar la clave privada.

4 Hay dos opciones para utilizar la clave pública:

- Guardar la clave pública en un archivo para cargarlo más tarde.
- Copiar y pegar el texto de la ventana **Clave pública para pegar** al agregar la cuenta mediante la opción de texto.

Generación de claves públicas para sistemas que ejecutan Linux

La aplicación ssh-keygen para los clientes Linux es una herramienta de línea de comandos sin interfaz gráfica de usuario. Abra una ventana de terminal y, al aparecer la solicitud de shell, escriba:

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

donde:

La opción `–t` debe 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.

La *passphrase* es opcional. Después de completar el comando, utilice el archivo público para pasar a RACADM y cargar el archivo.

Notas de la sintaxis de RACADM para CMC

Cuando utilice el comando `racadm sshpkauth`, asegúrese de cumplir estos requisitos:

- Para la opción `-i`, el parámetro debe ser `svcacct`. Todos los demás parámetros para `-i` fallan en la CMC. La `svcacct` es una cuenta especial para la autenticación de clave pública en SSH en la CMC.
- Para iniciar sesión en la CMC, el usuario debe ser servicio. Los usuarios de las demás categorías tienen acceso a las claves públicas introducidas mediante el comando. `sshpkauth`

Visualización de claves públicas

Para ver las claves públicas que se han agregado al CMC, escriba:

```
racadm sshpkauth -i svcacct -k all -v
```

Para ver una clave a la vez, reemplace `all` con un número de 1 a 6. Por ejemplo, para ver la clave 2, escriba:

```
racadm sshpkauth -i svcacct -k 2 -v
```

Adición de claves públicas

Para agregar una clave pública a la CMC mediante la opción de carga de archivos `-f`, en la consola de la interfaz de la línea de comandos, escriba:

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -f <public key file>
```

NOTA: Solo puede usar la opción de carga de archivos con RACADM remoto. Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Para agregar una clave pública mediante la opción de carga de texto, escriba:

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -t "<public key text>"
```

Eliminación de claves públicas

Para eliminar una clave pública, ejecute el siguiente comando:

```
racadm sshpkauth -i svcacct -k 1 -d
```

Para eliminar todas las claves públicas, ejecute el siguiente comando:

```
racadm sshpkauth -i svcacct -k all -d
```

Configuración del software de emulación de terminal

El CMC admite una consola de texto en serie de una estación de administración que ejecuta uno de los siguientes tipos de software de emulación de terminal:

- Minicom de Linux.
- HyperTerminal Private Edition (versión 6.3) de Hilgraeve.

Ejecute las tareas en las subsecciones siguientes para configurar el tipo de software de terminal necesario.

Configuración de Minicom de Linux

Minicom es una utilidad de acceso de puerto serie para Linux. Los siguientes pasos son válidos para configurar Minicom versión 2.0. Es posible que otras versiones de Minicom difieran un poco, pero requieren la misma configuración básica. Para configurar otras versiones de Minicom, consulte la información en la sección Configuración requerida de Minicom de esta Guía del usuario.

Configuración de Minicom versión 2.0

NOTA: Para obtener los mejores resultados, establezca la propiedad cfgSerialConsoleColumns para que coincida con el número de columnas. Tenga en cuenta que la petición ocupa dos caracteres. Por ejemplo, para una ventana de terminal con 80 columnas:

```
racadm config -g cfgSerial -o
cfgSerialConsoleColumns 80.
```

1. Si no tiene un archivo de configuración de Minicom, vaya al siguiente paso. Si tiene un archivo de configuración de Minicom, escriba `minicom<Minicom config file name>`) y, a continuación, vaya al paso 12.
2. En la petición de comandos de Linux, escriba `minicom -s`.
3. Seleccione **Configuración del puerto serie** y presione <Intro>.
4. Presione <a> y seleccione el dispositivo de serie correspondiente (por ejemplo, `/dev/ttyS0`).
5. Presione <e> y defina la opción **Bps/Par/Bits** con el valor **115200 8N1**.
6. Presione la tecla <f>, y, a continuación, establezca **Control de flujo de hardware** en **Sí** y **Control de flujo de software** en **No**. Para salir del menú **Configuración del puerto serie**, presione <Enter>).
7. Seleccione **Módem y marcación** y presione <Intro>.
8. En el menú **Configuración de parámetros y marcación de módem**, presione <Retroceso> para borrar los valores **init**, **reset**, **connect** y **hangup** de modo que queden en blanco; luego presione <Intro> para guardar cada valor en blanco.
9. Cuando se hayan borrado todos los campos especificados, presione <Intro> para salir del menú **Configuración de parámetros y marcación de módem**.
10. Seleccione **Salir de Minicom** y presione <Intro>.
11. Cuando aparezca la solicitud shell del comando, escriba `minicom <Minicom config file name>`.
12. Para salir de Minicom, presione <Ctrl><a>, <x>, <Intro>.

    Asegúrese de que la ventana Minicom muestre una solicitud de inicio de sesión. Cuando esta solicitud aparezca, la conexión se habrá completado con éxito. Ahora podrá iniciar sesión y obtener acceso a la interfaz de línea de comandos de la CMC.

Valores de Minicom necesarios

Consulte la siguiente tabla para configurar cualquier versión de Minicom.

Tabla 33. Configuración de Minicom

Descripción del valor	Valor necesario
Bps/Par/Bits	115200 8N1
Control de flujo de hardware	Sí
Control de flujo de software	No
Emulación de terminal	ANSI
Configuración de parámetros y marcación de módem	Borre los valores **init**, **reset**, **connect** y **hangup** de modo que queden en blanco.

Conexión a servidores o módulos de Entrada/Salida con el comando Connect

La CMC puede establecer una conexión para redirigir la consola serie del servidor o los módulos de E/S.

Para los servidores, la redirección de consola serie se puede llevar a cabo mediante:

- La interfaz de línea de comandos de la CMC (CLI) o el comando `connect` de RACADM. Para obtener más información sobre cómo usar comandos RACADM, consulte la *Guía de referencia sobre líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX*.
- La función de redirección de consola serie de la interfaz web del iDRAC.
- La función de comunicación en serie en la LAN (SOL) del iDRAC.

En una consola serie, Telnet o SSH, la CMC admite el comando `connect` para establecer una conexión serie con un servidor o módulo de E/S. La consola serie del servidor contiene las pantallas de inicio y configuración del BIOS y la consola serie del sistema operativo. En el caso del módulo de E/S, está disponible una consola serie del conmutador. En el chasis hay un solo módulo de E/S.

PRECAUCIÓN: Cuando se ejecuta desde la consola serie de la CMC, la opción `connect -b` permanece conectada hasta que se restablece la CMC. Esta conexión supone un posible riesgo de seguridad.

NOTA: El comando `connect` proporciona la opción `–b` (binaria). La opción `–b` transmite datos binarios sin procesar y `cfgSerialConsoleQuitKey` no se utiliza. Asimismo, al establecer conexión con un servidor por medio de la consola serie de la CMC, las transiciones en la señal DTR (por ejemplo, si se quita el cable serie para conectar un depurador) no causan una desconexión de la aplicación.

NOTA: Si el módulo de E/S no admite la redirección de consola, el comando `connect` muestra una consola vacía. En tal caso, para regresar a la consola de la CMC, escriba la secuencia de Escape. La secuencia de escape de la consola predeterminada es <Ctrl>< \ >.

Para conectarse a un módulo de E/S escriba:

```
connect switch-n
```

en donde `n` es un módulo de E/S con la etiqueta A1.

Cuando se hace referencia al módulo de E/S en el comando connect, el módulo se asigna a un conmutador como muestra la siguiente tabla.

Tabla 34. Asignación de módulos de E/S en conmutadores

Etiqueta del módulo de E/S	Conmutador
A1	switch-a1 o switch- 1

NOTA: Solo puede haber una conexión del módulo de E/S por chasis al mismo tiempo.

NOTA: No es posible establecer conexiones de paso desde la consola serie.

Para conectarse a una consola serie del servidor administrado, ejecute el comando `connect server-n`, donde *n* es 1-4. También se puede usar el comando `racadm connect server-n`. Cuando se conecta a un servidor por medio de la opción `–b`, se asume una comunicación binaria y el caracter de Escape se deshabilita. Si el iDRAC no está disponible, aparece el mensaje de error `No route to host`.

El comando `connect server-n` permite que el usuario obtenga acceso al puerto serie del servidor. Tras establecerse la conexión, el usuario podrá ver la redirección de consola del servidor a través del puerto serie de la CMC que incluye la consola serie del BIOS y la consola serie del sistema operativo.

NOTA: Para ver las pantallas de inicio del BIOS, es necesario activar la redirección de serie en la configuración del BIOS de los servidores. Además, se debe configurar la ventana del emulador terminal en 80x25. De lo contrario, los caracteres de la página no se mostrarán correctamente.

NOTA: No todas las teclas funcionan en las páginas de configuración del BIOS. Por lo tanto, brinde accesos directos de teclado para <Ctrl> <Alt> <Delete> y otros. La pantalla de redirección inicial muestra los atajos de teclado necesarios.

Configuración del BIOS del servidor administrado para la redirección de consola serie

Puede usar una sesión de consola remota para conectarse al sistema administrado mediante la interfaz web del iDRAC (consulte la *iDRAC User's Guide* (Guía del usuario de iDRAC) en **dell.com/support/manuals**).

La comunicación en serie del BIOS está desactivada de forma predeterminada. Para redirigir los datos de la consola de texto del host a la comunicación en serie en la LAN, se debe activar la redirección de la consola a través de COM1. Para cambiar la configuración del BIOS:

1 Encienda el servidor administrado.

2 Presione <F2> para acceder a la utilidad de configuración del BIOS durante la autoprueba de encendido.

3 Vaya a **Comunicación en serie** y, a continuación, presione <Enter> . En el cuadro de diálogo, la lista de comunicación en serie muestra las siguientes opciones:

- **desactivado**
- **Encendido sin redirección de consola**
- **Encendido con redirección de consola a través de COM1**

Para navegar entre estas opciones, presione las teclas de flechas correspondientes.

NOTA: Asegúrese de seleccionar la opción Encendido con redirección de consola a través de COM1.

4 Active **Redirección después de inicio** (el valor predeterminado es **desactivado**). Esta opción permite la redirección de la consola del BIOS en inicios posteriores.

5 Permite guardar los cambios y salir.

El sistema administrado se reiniciará.

Configuración de Windows para la redirección de consola en serie

No es necesario configurar los servidores que ejecutan versiones de Microsoft Windows Server, a partir de Windows Server 2003. Windows recibirá información del BIOS y activará la Consola de administración especial (SAC) COM1.

Configuración de Linux para la redirección de la consola en serie del servidor durante el inicio

Los pasos siguientes se aplican a Linux GRand Unified Bootloader (GRUB). Se deben realizar cambios similares si se utiliza un cargador de inicio diferente.

NOTA: Al configurar la ventana de emulación del cliente VT100, defina la ventana o aplicación que muestra la consola redirigida en 25 filas por 80 columnas para garantizar que se muestre el texto correctamente. De lo contrario, algunas pantallas de texto pueden aparecer distorsionadas.

Modifique el archivo **/etc/grub.conf** según se indica a continuación:

1 Localice las secciones de configuración general en el archivo y agregue las siguientes dos líneas nuevas:

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2 Anexe dos opciones a la línea de núcleo:

```
kernel console=ttyS1,57600
```

3 Si el archivo **/etc/grub.conf** contiene una directiva `splashimage`, inserte un carácter de comentario al inicio de la línea para anularla.

El siguiente ejemplo ilustra los cambios descritos en este procedimiento.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making
changes
# to this file
# NOTICE: You do not have a /boot partition. This
means that
# all kernel and initrd paths are relative to
/, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=
/dev/sda1
# initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial
title Red Hat Linux Advanced Server (2.4.9-e.3smp)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=
/dev/sda1 hda=ide-scsi console=ttyS0 console=
ttyS1,57600
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1
initrd /boot/initrd-2.4.9-e.3.img
```

Cuando edite el archivo **/etc/grub.conf**, siga estas pautas:

- Desactive la interfaz gráfica de GRUB y utilice la interfaz basada en texto. De lo contrario, la pantalla GRUB no se mostrará en la redirección de la consola. Para desactivar la interfaz gráfica, inserte un caracter de comentario en la línea que comienza con `splashimage`
- Para abrir varias opciones de GRUB a fin de iniciar sesiones de consola por medio de la conexión en serie, agregue la siguiente línea a todas las opciones:

  ```
  console=ttyS1,57600
  ```

  El ejemplo muestra el elemento `console=ttyS1,57600`agregado sólo a la primera opción.

Configuración de Linux para la redirección de consola serie del servidor después del inicio

Edite el archivo **/etc/inittab**, como se indica a continuación:

Agregue una nueva línea para configurar `agetty` en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1
ansi
```

El siguiente ejemplo muestra el archivo con la nueva línea.

```
#
# inittab This file describes how the INIT process
# should set up the system in a certain
# run-level.
#
# Author: Miquel van Smoorenburg
# Modified for RHS Linux by Marc Ewing and
# Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you
# do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
# Things to run in every runlevel.
ud::once:/sbin/update
# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
# When our UPS tells us power has failed, assume we
have a few
# minutes of power left. Schedule a shutdown for 2
minutes from now.
# This does, of course, assume you have power
installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure;
System Shutting Down"
# If power was restored before the shutdown kicked in,
cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power
Restored; Shutdown Cancelled"
# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Edite el archivo **/etc/securetty** de la siguiente manera:

Agregue una nueva línea, con el nombre del tty serie para COM2:

```
ttyS1
```

El siguiente ejemplo muestra un archivo con la nueva línea.

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

12

Uso de FlexAddress y FlexAddress Plus

En esta sección se proporciona información acerca de FlexAddress, FlexAddress Plus y configuración.

NOTA: Se debe instalar una licencia Enterprise en el CMC para poder utilizar la función FlexAddress.

Temas:

Acerca de FlexAddress

Si se reemplaza un servidor, la función FlexAddress de la ranura sigue siendo igual para la ranura del servidor dado. Si el servidor se inserta en una nueva ranura o un nuevo chasis, se utiliza la dirección WWN/MAC asignada por el servidor a menos que el chasis particular tenga la función FlexAddress activada para la ranura nueva. Si quita el servidor, regresará a la dirección asignada por el servidor. No es necesario volver a configurar los marcos de implementación, los servidores DHCP y los enrutadores de diversas redes Fabric para identificar el servidor nuevo.

A cada módulo del servidor se le asignan direcciones WWN y/o MAC exclusivas como parte del proceso de fabricación. Sin FlexAddress, si tiene que reemplazarse un servidor con otro módulo de servidor, las direcciones WWN/MAC cambian y las herramientas de administración de red Ethernet y los recursos SAN tienen que volver a configurarse para identificar el nuevo módulo del servidor.

FlexAddress permite que la CMC asigne direcciones WWN/MAC a una ranura determinada y sobrescriba las direcciones de fábrica. Si se sustituye el módulo del servidor, las direcciones WWN/MAC basadas en ranuras no cambian. Gracias a esta función, ya no es necesario volver a configurar las herramientas de administración de la red Ethernet y los recursos SAN para un nuevo módulo de servidor.

Asimismo, la acción *sustituir* solo se produce cuando se inserta un módulo de servidor en un chasis compatible con FlexAddress; no se realizan cambios permanentes en el módulo de servidor. Si se mueve un módulo de servidor a un chasis que no admite FlexAddress, se utilizan las direcciones WWN/MAC asignadas de fábrica.

El chasis VRTX de la CMC se envía con la tarjeta SD, que admite las funciones FlexAddress, FlexAddress Plus y Almacenamiento extendido. Si el chasis VRTX se suministra con una segunda CMC opcional, esta tiene una tarjeta SD que únicamente admite el almacenamiento extendido.

NOTA:

- La información contenida en la tarjeta SD está cifrada y no es posible duplicarla o alterarla de ninguna forma porque podría desactivar las funciones del sistema y ocasionar que el sistema deje de funcionar.
- El uso de una tarjeta SD se limita a un solo chasis. No puede utilizar la misma tarjeta SD en otro chasis.

La tarjeta de función FlexAddress contiene un rango de direcciones MAC. Antes de instalar FlexAddress, puede determinar el rango de direcciones MAC contenidas en una tarjeta de función FlexAddress insertando la tarjeta SD en un Lector de tarjetas de memoria USB y

visualizando el archivo **pwwn_mac.xml**. Este archivo XML de texto no cifrado de la tarjeta SD contiene una etiqueta XML *mac_start* que es la primera dirección MAC hex. inicial que se utiliza para este rango exclusivo de direcciones MAC. La etiqueta *mac_count* es el número total de direcciones MAC que asigna la tarjeta SD. El rango total de direcciones MAC asignadas se puede determinar de la manera siguiente:

```
<mac_start> + <mac_count>  - 1 = <mac_end>
```

Por ejemplo:

```
(starting_mac)00188BFFDCFA + (mac_count)0xCF - 1 = (ending_mac)00188BFFDDC8
```

.

NOTA: Bloquee la tarjeta SD antes de insertarla en el Lector de tarjetas de memoria USB para evitar modificar accidentalmente el contenido. Debe desbloquear la tarjeta SD antes de insertarla en la CMC.

Acerca de FlexAddress Plus

FlexAddress Plus es una nueva función que se agrega a la versión 2.0 de la tarjeta de función. Se trata de una actualización de la tarjeta de función FlexAddress versión 1.0. La función FlexAddressPlus contiene más direcciones MAC que FlexAddress. Ambas funciones permiten que el chasis asigne direcciones de Nombre mundial/Control de acceso de medios (WWN/MAC) a dispositivos Fibre Channel y Ethernet. Las direcciones WWN/MAC asignadas por el chasis son únicas a nivel mundial y específicas de una ranura de servidor.

Visualización del estado de activación de FlexAddress

Una tarjeta de función que contiene una o más de las siguientes funciones: FlexAddress, FlexAddress Plus y/o almacenamiento extendido.

Para ver el estado de FlexAddress del chasis mediante la interfaz web del CMC, vaya a **Descripción general del chasis** > **Configuración**.

Aparecerá la página **Configuración general del chasis**.

La función **FlexAddress** tiene un valor **Activo** o **No activo**. El valor **Activo** indica que la función está instalada en el chasis, mientras que **No activo** indica que la función no está instalada y no está en uso en el chasis.

Ejecute el siguiente comando de RACADM para ver el estado de la tarjeta de función SD:

```
racadm featurecard -s
```

Aparece el siguiente mensaje:

```
Active CMC:
The feature card inserted is valid, serial number CN0H871T1374036T00MXA00
The feature card contains the following feature(s)
       FlexAddress: bound
       FlexAddressPlus: bound
       ExtendedStorage: bound
Standby CMC:
The feature card contains the following feature(s)
       ExtendedStorage: bound
```

NOTA: El CMC secundario es opcional y el resultado para el CMC en espera se muestra solamente si el CMC en espera está disponible en el chasis.

Tabla 35. Mensajes de estado que muestra el comando featurecard -s

Mensaje de estado	Acciones
`No feature card inserted.`	Revise la CMC para verificar que la tarjeta SD se ha insertado correctamente. En una configuración redundante de la CMC,

Mensaje de estado	Acciones
	asegúrese de que la CMC con la tarjeta de función SD instalada sea la CMC activa y no la CMC en espera.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound.`	No es necesario realizar ninguna acción.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.`	Retire la tarjeta SD; coloque e instale la tarjeta SD en el chasis actual.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.`	La tarjeta de función se puede pasar a otro chasis o se puede reactivar en el chasis actual. Para reactivarla en el chasis actual, introduzca `racadm racreset` hasta que el módulo de la CMC con la tarjeta de función instalada se active.

Use el siguiente comando de RACADM para mostrar todas las funciones activadas en el chasis:

```
racadm feature -s
```

El comando produce el mensaje de estado siguiente:

```
Feature Name = FlexAddress
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = FlexAddressPlus
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = ExtendedStorage
       Current Status = redundant, active
       Date/time Activated = 05 Oct 2013 - 11:50:58
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00
```

Si no hay funciones activas en el chasis, el comando mostrará un mensaje:

```
racadm feature -s
No features active on the chassis
```

Las tarjetas de funciones de Dell pueden contener más de una función. Una vez activada cualquiera de las funciones incluidas en la Tarjeta de funciones de Dell en un chasis, las demás funciones que se puedan incluir en esa Tarjeta de funciones de Dell no se podrán activar en un chasis diferente. En este caso, el comando `racadm feature -s` muestra el siguiente mensaje para las funciones afectadas:

```
ERROR: One or more features on the SD card are active on another chassis
```

Para obtener más información acerca de los comandos `feature` y `featurecard`, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en el sitio de asistencia.

Configuración de FlexAddress

FlexAddress es una actualización opcional que permite a los módulos de los servidores reemplazar la dirección WWN/MAC asignada de fábrica por una dirección WWN/MAC proporcionada por el chasis.

NOTA: En esta sección, el término FlexAddress también hace referencia a FlexAddress Plus.

NOTA: Con el subcomando `racresetcfg` puede restablecer la FlexAddress de una CMC a su configuración predeterminada de fábrica que está "desactivada". La sintaxis de RACADM es:

```
racadm racresetcfg -c flex
```

Para obtener más información sobre los comandos RACADM relacionados con FlexAddress y los datos de otras propiedades predeterminadas de fábrica, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en dell.com/cmcmanuals.

El servidor debe estar apagado para iniciar la configuración. Puede activar o desactivar FlexAddress en cada red Fabric. Otra opción es activar o desactivar la función en cada ranura. Después de activarla en cada red Fabric, puede seleccionar la activación de las ranuras. Por ejemplo, si la red Fabric A está activada, todas las ranuras que estén activadas tendrán FlexAddress activado solo en la red Fabric A. El resto de las redes Fabric utilizará la WWN/MAC asignada de fábrica en el servidor.

NOTA: FlexAdress no tiene efecto en un módulo de servidor hasta el siguiente reinicio. Cuando se implementa la función FlexAddress por primera vez en un módulo del servidor, se requiere de una secuencia de apagado y encendido para que FlexAddress se active. FlexAddress en dispositivos Ethernet se programa por el BIOS del módulo del servidor. Para que el BIOS del módulo del servidor programe la dirección, necesita estar en funcionamiento, lo que requiere que el módulo del servidor se encienda. Cuando se completan las secuencias de apagado y encendido, las direcciones MAC asignadas por el chasis estarán disponibles para la función de encendido en LAN (WOL).

Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis

En el nivel del chasis, puede activar o desactivar la función FlexAddress para redes Fabric y ranuras. FlexAddress se activa para cada red Fabric y, después, se seleccionan las ranuras que deben participar en la función. Tanto las redes Fabric como las ranuras deben activarse para configurar FlexAddress satisfactoriamente.

Configuración de FlexAddress para redes Fabric y ranuras en el nivel del chasis mediante la interfaz web del CMC

Si un servidor está presente en la ranura, apáguelo antes de activar la función FlexAddress en esa ranura.

Para activar o desactivar redes Fabric y ranuras para usar la función de FlexAddress mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en**Descripción general del servidor** > **Configuración** > **FlexAddress**.
2. En la página **Implementar FlexAddress**, en la sección **Seleccionar redes Fabric para las direcciones WWN/MAC asignadas al chasis**, seleccione el tipo de red Fabric (**Fabric-A** o **iDRAC**) para el cual desea activar FlexAddress. Para desactivar esta función, desactive la opción.
3. En la página **Seleccionar ranuras para las direcciones WWN/MAC asignadas al chasis**, seleccione la opción **Activado** para la ranura donde desea activar FlexAddress. Para desactivar esta función, desactive la opción.

   NOTA: Tenga en cuenta lo siguiente:

   - Si no se selecciona ninguna ranura, FlexAddress no se activa para la red Fabric seleccionada.
   - Si no se selecciona ninguna de las redes Fabric y se selecciona y aplica una ranura de servidor, aparece el siguiente mensaje `No fabrics selected! FlexAddress will not be used on this chassis.` Seleccione la red Fabric y la ranura para configurar FlexAddress satisfactoriamente.
   - No se permite configurar FlexAddress para una ranura esclava. La opción aparece atenuada en la interfaz web de la CMC. Los dispositivos de Ethernet asociados con la ranura esclava del servidor heredan la configuración de la ranura maestra.
4. Para guardar la configuración, haga clic en **Aplicar**.

Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis mediante RACADM

Para activar o desactivar las redes Fabric, use el siguiente comando RACADM:

```
racadm setflexaddr [-f <fabricName> <state>]
```

donde, `<fabricName> = A or iDRAC` y `<state> = 0 or 1`

El valor 0 es desactivar y 1 es activar.

Para activar o desactivar las ranuras, use el siguiente comando RACADM:

```
racadm setflexaddr [-i <slot#> <state>
```

donde, `<slot#> = 1 or 4` y `<state> = 0 or 1`

El valor 0 es desactivar y 1 es activar.

Para obtener más información acerca del comando **setflexaddr**, consulte la *Guía de referencia sobre línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX*.

NOTA: Si adquiere la función FlexAddress o FlexAddressPlus con Dell PowerEdge VRTX, este viene preinstalado y activado para todas las ranuras y redes Fabric. Para adquirir esta función, comuníquese con Dell en dell.com.

NOTA: Con el subcomando `racresetcfg` puede restablecer la FlexAddress de una CMC a su configuración predeterminada de fábrica que está "desactivada". La sintaxis de RACADM es:

```
racadm racresetcfg -c flex
```

Para obtener más información sobre los comandos RACADM relacionados con FlexAddress y los datos de otras propiedades predeterminadas de fábrica, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en dell.com/cmcmanuals.

Visualización de direcciones de nombre mundial (WWN) o Control de acceso a medios

La página **Resumen de WWN/MAC** permite ver la configuración de Nombre mundial (WWN) y la dirección de Control de acceso a medios (MAC) de una ranura en el chasis.

Configuración de la red Fabric

La sección **Configuración de la red Fabric** muestra el tipo de red Fabric de entrada/salida que se instala para la red Fabric A. Una marca verde indica que la red Fabric está activada para FlexAddress. La función FlexAddress se utiliza para instalar direcciones WWN/MAC persistentes de ranuras y asignadas por el chasis en varias redes Fabric y ranuras en el chasis. Esta función se activa según la red Fabric y la ranura.

NOTA: Para obtener más información acerca de la función FlexAddress, consulte Acerca de FlexAddress.

Visualización de la información de la dirección WWN o MAC

Puede ver el inventario de las direcciones WWW/MAC de los adaptadores de red para cada ranura de servidor o para todos los servidores en el chasis. El inventario incluye lo siguiente:

- Configuración de la red Fabric

  NOTA:
  - La red Fabric A muestra el tipo de red Fabric de entrada/salida instalado. Si está activada la red Fabric A, las ranuras que no están ocupadas muestran las direcciones MAC asignadas al chasis para la red Fabric A.
  - La controladora de administración de iDRAC no es una red Fabric, pero su FlexAddress es considerado como tal.
  - SI la casilla de verificación asociada con un componente está seleccionada, significa que la red Fabric está activada para FlexAddress o FlexAddressPlus.
- Protocolo que se utiliza en el puerto del adaptador NIC. Por ejemplo, LAN, ISCI y FCoE.
- La configuración del nombre mundial (WWN) de Fiber Channel y las direcciones de control de acceso de medios (MAC) de una ranura en el chasis.
- Tipo de asignación de la dirección MAC y tipo de dirección activa actualmente: asignada por el servidor, FlexAddress o MAC de la identidad de E/S. Una marca negra indica el tipo de dirección activa, ya sea asignada por el servidor, por el chasis o de manera remota.
- Estado de las particiones de NIC para los dispositivos que admite la creación de particiones.

Puede ver el inventario de direcciones WWN/MAC a través de la interfaz web o la CLI de RACADM. Basándose en la interfaz, puede filtrar la dirección MAC y saber qué dirección WWN/MAC está en uso para esa función o partición. Si el adaptador tiene NPAR activado, puede ver qué particiones están activadas o desactivadas.

Mediante la interfaz web, puede ver la información de direcciones WWN/MAC para:

- Ranuras específicas: abra la página **FlexAddress**. Para ello, haga clic en **Descripción general del servidor** > **Ranura <x>** > **Configuración** > **FlexAddress**.
- Todas las ranuras y el servidor: abra la página **Resumen de WWN/MAC** . Para ello, haga clic en **Descripción general del servidor** > **Propiedades** > **WWN/MAC**.

Desde ambas páginas puede ver la información de Direcciones WWN/MAC en el modo básico o en el modo avanzado:

- **Modo básico**: en este modo, puede ver Ranura del servidor, Red Fabric, Protocolo, Direcciones WWN/MAC y Estado de la partición. Solo las direcciones MAC activas se muestran en la casilla de direcciones WWN/MAC. Puede filtrar mediante cualquiera o todos los campos que aparecen en pantalla.
- **Modo avanzado**: en este modo, puede ver todos los campos que se muestran en el modo básico y todos los tipos de MAC (asiganda por el servidor, asignada por Flex Address e identidad de E/S). Puede filtrar mediante cualquiera o todos los campos que aparecen en pantalla.

En el modo básico y el modo avanzado, la información de las Direcciones WWN/MAC se muestra en formato contraído. Haga clic en el símbolo del ⊞ correspondiente a una ranura o haga clic en **Expandir/Contraer todos** para ver la información de una ranura específica o de todas las ranuras.

También puede exportar la información de las direcciones WWN/MAC para todos los servidores del chasis en una carpeta local.

Para obtener información acerca de los campos, consulte la *ayuda en línea*.

Visualización de la información básica de las direcciones WWN o MAC mediante la interfaz web

Para ver la información de las direcciones WWN/MAC para cada ranura de servidor o todos los servidores del chasis en el modo básico:

1 Haga clic en **Descripción general del servidor** > **Propiedades** > **WWN/MAC**

La página **Resumen de WWN/MAC** muestra la información sobre las direcciones WWN/MAC.

De manera alternativa, haga clic en **Descripción general del servidor** > **Ranura <x>** > **Configuración** > **FlexAddress** para ver la información de la dirección WWN/MAC de una ranura del servidor específica. Aparecerá la página **FlexAddress**.

2 En la tabla **Direcciones WWN/MAC** , haga clic en **Exportar** para guardar las direcciones WWN/MAC localmente.

3 Haga clic en el correspondiente a una ranura o haga clic en **Expandir/Contraer todo** para expandir o contraer la lista de atributos de una ranura específica o de todas las ranuras en la tabla Direcciones WWN/MAC.

4 En el menú desplegable **Ver**, seleccione **Básico** para ver los atributos de las direcciones WWN/MAC en la vista de árbol.

5 En el menú desplegable **Ranura del servidor** , seleccione **Todos los servidores** o una ranura específica para ver los atributos de las direcciones WWN/MAC para todos los servidores o solo para servidores en ranuras específicas, respectivamente.

6 En el menú desplegable **Red Fabric**, seleccione uno de los tipos de red Fabric para ver los detalles de todos los tipos o de tipos específicos de administración o redes Fabric de E/asociadas con los servidores.

7 Desde el menú desplegable **Protocolo**, seleccione **Todos los protocolos** o uno de los protocolos de red de la lista para ver todos los MACS o las direcciones MAC asociadas con el protocolo seleccionado.

8 En el campo **Direcciones WWN/MAC**, introduzca una dirección MAC parcial o toda la dirección MAC para ver únicamente las ranuras asociadas con la dirección MAC específica.

9 En el menú desplegable **Estado de la partición**, seleccione el estado de las particiones para visualizar los servidores con el estado de la partición seleccionado.

Para obtener información acerca de los campos, consulte la *ayuda en línea*.

Visualización de la información avanzada de las direcciones WWN o MAC mediante la interfaz web

Para ver información sobre las direcciones WWN/MAC para cada ranura de servidor o todos los servidores del chasis en el modo avanzado:

1 Haga clic en **Descripción general del servidor** > **Propiedades** > **WWN/MAC**

La página **Resumen de WWN/MAC** muestra la información sobre las direcciones WWN/MAC.

2 En el menú desplegable **Ver** , seleccione **Opciones avanzadas** para ver los atributos de las direcciones WWN/MAC en la vista detallada.

En la tabla **Direcciones WWN/MAC** se muestra la Ranura del servidor, la red Fabric, el protocolo, las direcciones WWN/MAC, el estado de la partición y el tipo de asignación de la dirección de MAC: asignada por el servidor, FlexAddress o MAC de identidad de E/S. Una marca negra indica el tipo de dirección activa, ya sea asignada por el servidor, por el chasis o de manera remota. MAC.

3 En la tabla **Direcciones WWN/MAC** , haga clic en **Exportar** para guardar las direcciones WWN/MAC localmente.

4 Haga clic en el en una ranura o haga clic en **Expandir/contraer todos** para expandir o contraer los atributos de la lista para una ranura específica o para todas las ranuras en la tabla Direcciones WWN/MAC.

5 En el menú desplegable **Ranura del servidor** , seleccione **Todos los servidores** o una ranura específica para ver los atributos de las direcciones WWN/MAC para todos los servidores o solo para servidores en ranuras específicas, respectivamente.

6 En el menú desplegable **Red Fabric**, seleccione uno de los tipos de red Fabric para ver los detalles de todos los tipos o de tipos específicos de administración o redes Fabric de E/asociadas con los servidores.

7 Desde el menú desplegable **Protocolo**, seleccione **Todos los protocolos** o uno de los protocolos de red de la lista para ver todos los MACS o las direcciones MAC asociadas con el protocolo seleccionado.

8 En el campo **Direcciones WWN/MAC**, introduzca la dirección MAC para ver únicamente las ranuras asociadas con la dirección MAC específica.

9 En el menú desplegable **Estado de la partición**, seleccione el estado de las particiones para visualizar los servidores con el estado de la partición seleccionado.

Si una partición en particular está desactivada, el estado se muestra como **Desactivado** y la fila que muestra la partición aparece atenuada.

Para obtener información acerca de los campos, consulte la *ayuda en línea*.

Visualización de la información de direcciones WWN o MAC mediante RACADM

Para ver la información de las direcciones WWN/MAC para todos los servidores o servidores específicos mediante RACADM, utilice los subcomandos `getflexaddr` y `getmacaddress`.

Para mostrar Flexaddress para todo el chasis, utilice el siguiente comando RACADM:

```
racadm getflexaddr
```

Para ver el estado de FlexAddress para una ranura particular, utilice el siguiente comando de RACADM:

```
racadm getflexaddr [-i <slot#>]
```

donde *<número de ranura>* es un valor de 1 a 4.

Para ver la dirección MAC de la LOM o NDC, utilice el siguiente comando de RACADM:

```
racadm getmacaddress
```

Para ver la dirección MAC del chasis, utilice el siguiente comando RACADM:

```
racadm getmacaddress -m chassis
```

Para ver las direcciones MAC de iSCSI de todos los servidores, utilice el siguiente comando de RACADM:

```
racadm getmacaddress -t iscsi
```

Para ver las MAC de iSCSI para un servidor específico, utilice el siguiente comando de RACADM:

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

Para ver la dirección MAC y WWN definida por el usuario, utilice el siguiente comando de RACADM:

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

Para ver la MAC/WWN asignada por la consola de todas las LOM o tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c all
```

Para ver la dirección asignada WWN/MAC del chasis, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c flexaddress
```

Para ver la direcciones MAC/WWN para todas las LOM o tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c factory
```

Para ver las direcciones MAC/WWN de iSCSI y Ethernet para todos los iDRAC/LOM/tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -a
```

Para obtener más información acerca de los subcomandos **getflexaddr** y **getmacaddress**, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX).

Mensajes de comandos

En la siguiente tabla se muestran los comandos RACADM y los mensajes de situaciones comunes de FlexAddress.

Tabla 36. Comandos y mensajes de salida de FlexAddress

Situación	Comando	Salida

La tarjeta SD en el módulo CMC activo está vinculada a otra etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`

La tarjeta SD en el módulo CMC activo está vinculada a la misma etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: bound`

La tarjeta SD en el módulo CMC activo no está vinculada a ninguna etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress:not bound`

Función FlexAddress no activada en el chasis por algún motivo (no hay tarjeta SD insertada, tarjeta SD dañada, después haber desactivado la función, tarjeta SD vinculada a otro chasis).	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		`ERROR: Flexaddress feature is not active on the chassis`

El usuario invitado intenta configurar FlexAddress en ranuras/redes Fabric.	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		`ERROR: Insufficient user privileges to perform operation`

Desactivar la función FlexAddress con el chasis encendido.	`$racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON`
El usuario invitado intenta desactivar la función en el chasis.	`$racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation`
Cambiar la configuración de FlexAddress de ranuras/redes Fabric mientras los módulos del servidor están encendidos.	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`

Cambio de la configuración de Flexaddress en ranuras o redes Fabric cuando no hay instalada una licencia CMC Enterprise.	`$racadm setflexaddr -i<slotnum> <status>`
	
	`$racadm setflexaddr -f<FabricName> <status>`
		`ERROR: SWC0242 : A required license is missing or expired. Obtain an appropriate license and try again, or contact your service provider for additional details.`

Situación	Comando	Salida

NOTA: Para solucionar este problema, debe contar con una licencia de Activación de FlexAddress.

CONTRATO DE LICENCIA DE SOFTWARE DE DELL FlexAddress

El presente documento es un contrato legal entre usted, el usuario, y Dell Products, L.P. o Dell Global B.V. ("Dell"). Este contrato cubre todo el software que se distribuye con el producto Dell, para el que no existe un contrato de licencia por separado entre usted y el fabricante o el propietario del software (conjuntamente, el "Software"). Este contrato no es para la venta de Software ni cualquier otra propiedad intelectual. Todos los derechos de título y propiedad intelectual del Software pertenecen al fabricante o el propietario del Software. Todos los derechos no otorgados expresamente en virtud de este contrato se reservan por el fabricante o propietario del Software. Al abrir o romper el sello de los paquetes de Software, instalar o descargar el Software, o utilizar el Software cargado previamente o incluido en el producto, usted acepta quedar sujeto a los términos de este contrato. Si no acepta estos términos, devuelva de inmediato todos los elementos de Software (discos, material escrito y embalaje) y elimine todo Software cargado previamente o incluido.

Puede utilizar una copia del Software solamente en un equipo a la vez. Si dispone de varias licencias de Software, podrá utilizar tantas copias a la vez como licencias posea. Por "utilizar", se entiende cargar el Software en la memoria temporal o en el almacenamiento permanente del equipo. La instalación en un servidor de red únicamente con motivos de distribución a otros equipos no implica "utilizar" si (aunque solo si) usted dispone de una licencia diferente para cada equipo al que se haya distribuido el Software. Debe asegurarse de que el número de personas que utilizan el Software instalado en un servidor de red no sea superior al número de licencias de las que dispone. Si el número de usuarios del Software instalado en un servidor de red supera el número de licencias, deberá adquirir licencias adicionales hasta que la cantidad de licencias equivalga a la cantidad de usuarios, antes de permitir que otros usuarios utilicen el Software. Si usted es un cliente comercial de Dell o un socio de Dell, por el presente concede a Dell, o a un representante seleccionado por Dell, el derecho a realizar una auditoría del uso del Software durante el horario laboral normal, acepta cooperar con Dell en dicha auditoría y proporcionarle todos los registros relacionados razonablemente con el uso que usted hace del Software. La auditoría se limitará a la verificación del cumplimiento de los términos de este contrato por su parte.

El Software está protegido por las leyes de derechos de autor de Estados Unidos y por tratados internacionales. Podrá realizar una copia del Software únicamente con motivos de copia de seguridad o archivado, o transferirlo a un único disco duro, siempre y cuando conserve el original únicamente con motivos de copia de seguridad o archivado. No podrá alquilar o arrendar el Software 240 mediante las tarjetas FlexAddress y FlexAddress Plus, ni copiar el material escrito que viene con el mismo, pero sí podrá transferir el Software y todos los materiales adjuntos de manera permanente como parte de la venta o transferencia del producto Dell, siempre y cuando no se quede con ninguna copia y los destinatarios acepten los términos del presente. Toda transferencia deberá incluir la actualización más reciente y todas las versiones anteriores. No se permite aplicar técnicas de ingeniería inversa, descompilar o desensamblar el Software. Si el paquete que viene junto con su equipo contiene discos compactos, discos de 3,5" o de 5,25", podrá utilizar únicamente los adecuados para su equipo. No podrá utilizar los discos en otro equipo o red, ni prestarlos, alquilarlos, arrendarlos o transferirlos a otro usuario, excepto en los casos permitidos en el presente contrato.

GARANTÍA LIMITADA

Dell garantiza que los discos de Software no presentarán defectos en materiales ni de fabricación, siempre que se realice un uso normal, durante noventa (90) días a partir de la fecha de recepción. Esta garantía se limita a usted y no es transferible. Las garantías implícitas se limitan a noventa (90) días a partir de la fecha de recepción del Software. Algunas jurisdicciones no permiten límites de vigencia de una garantía implícita, de modo que esta limitación puede no aplicarse en su caso. La responsabilidad total de Dell y de sus proveedores, así como su recurso exclusivo, se limitarán a (a) el reembolso del importe abonado por el Software o (b) la sustitución de los discos que no cumplan con los requisitos de esta garantía y que usted envíe a Dell con un número de autorización de devolución, por su cuenta y riesgo. Esta garantía limitada quedará nula si el disco se daña como resultado de un accidente, abuso, aplicación no adecuada o servicio o modificación por parte de alguna persona ajena a Dell. La garantía cubre los discos de reemplazo durante el período restante de la garantía original o por treinta (30) días, según el período que resulte mayor.

Dell NO garantiza que las funciones del Software satisfarán sus necesidades o que el funcionamiento del Software no se interrumpirá o no tendrá errores. Usted asume la responsabilidad de seleccionar el Software para obtener los resultados esperados, así como del uso y los resultados obtenidos con el Software.

DELL, EN SU NOMBRE Y EN EL DE SUS PROVEEDORES, RENUNCIA A CUALQUIER OTRA GARANTÍA, EXPRESA O IMPLÍCITA, INCLUIDAS, SIN LIMITACIONES, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN PROPÓSITO DETERMINADO, EN LO QUE SE REFIERE AL SOFTWARE Y A TODOS LOS MATERIALES ESCRITOS ADJUNTOS CON EL MISMO. Esta garantía limitada le otorga derechos legales específicos, pero podrá disfrutar de otros en función de su jurisdicción.

EN NINGÚN CASO DELL O SUS PROVEEDORES SERÁN RESPONSABLES DE LOS DAÑOS QUE PUEDAN OCURRIR (LO QUE INCLUYE, SIN LIMITACIONES, LOS DAÑOS POR PÉRDIDA DE BENEFICIOS COMERCIALES, INTERRUPCIÓN O PÉRDIDA DE INFORMACIÓN DEL NEGOCIO O CUALQUIER OTRA PÉRDIDA PECUNIARIA) A CAUSA DEL USO O LA INCAPACIDAD DE UTILIZAR EL SOFTWARE, AUNQUE SE LE NOTIFIQUE DE LA POSIBILIDAD DE TALES DAÑOS. Puesto que algunas jurisdicciones no permiten la exclusión o limitación de responsabilidad por daños resultantes o accidentales, la limitación anteriormente mencionada puede no ser aplicable en su caso.

SOFTWARE DE CÓDIGO DE FUENTE ABIERTO

Una parte de este CD puede contener software de código de fuente abierto, que puede utilizar bajo los términos y condiciones de la licencia específica bajo la cual el software se distribuye.

ESTE SOFTWARE DE CÓDIGO DE FUENTE ABIERTO SE DISTRIBUYE CON LA INTENCIÓN DE QUE PUEDA SER ÚTIL, PERO SE PROPORCIONA "TAL CUAL" SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA; INCLUIDA, PERO SIN LIMITARSE A, LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO DELL, LOS TITULARES DE LOS DERECHOS DE AUTOR O COLABORADORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INHERENTE, ESPECIAL, EJEMPLAR O CONSIGUIENTE (LO QUE INCLUYE, SIN LIMITACIÓN, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS, O LA INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL), CUALQUIERA FUESE LA CAUSA Y EN CUALQUIER PRINCIPIO DE RESPONSABILIDAD, YA SEA EN VIRTUD DE CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUSO NEGLIGENCIA U OTRO) QUE SURJAN DEL USO DE ESTE SOFTWARE, INCLUSO SI SE ADVIERTE LA POSIBILIDAD DE TALES DAÑOS.

DERECHOS LIMITADOS DEL GOBIERNO DE EE. UU.

El software y la documentación son "artículos comerciales", tal como se define dicho término en 48 C.F.R. 2.101; es decir, "software informático comercial" y "documentación de software informático comercial", tal como se utilizan dichos términos en 48 C.F.R. 12.212. De conformidad con 48 C.F.R. 12.212 y 48 C.F.R. de 227.7202-1 a 227.7202-4, todos los usuarios finales del gobierno de EE. UU. adquieren el software y la documentación únicamente con los derechos estipulados en este documento.

El contratante/fabricante es Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

GENERAL

Esta licencia estará en vigor hasta que finalice. Dicha finalización tendrá lugar si se presentan las condiciones estipuladas anteriormente o si usted no cumple alguno de estos términos. Una vez finalizada, usted acepta que procederá a la destrucción del Software y de los materiales adjuntos, así como de todas las copias de estos. Este contrato está regulado por las leyes del estado de Texas. Cada cláusula de este contrato es independiente. Si se considera que alguna cláusula no es aplicable, dicha consideración no afectará la aplicabilidad del resto de las cláusulas, términos o condiciones de este contrato. Este contrato es vinculante para todos los sucesores y cesionarios. Tanto Dell como usted aceptan renunciar, en la medida máxima permitida por la ley, a cualquier derecho a un proceso con jurado con respecto al Software o este contrato. Debido a que esta renuncia de derechos puede no ser efectiva en ciertas jurisdicciones, es posible que no se aplique en su caso. Usted reconoce haber leído el presente contrato, haberlo entendido y quedar sujeto a sus términos, y que esta es la declaración completa y exclusiva del contrato entre usted y Dell con respecto al Software.

13

Administración de redes Fabric

El chasis admite el tipo de red Fabric A. Esta red es utilizada por el único módulo de E/S y está siempre conectada a los adaptadores Ethernet integrados de los servidores.

El chasis cuenta con un solo módulo de E/S (IOM), que funciona como módulo de paso o conmutación. El módulo de E/S se clasifica en el grupo A.

El módulo de E/S del chasis utiliza una ruta de acceso a datos discreta denominada **Red Fabric**, la cual recibe el nombre A. La red Fabric A admite solo Ethernet. Cada adaptador de E/S del servidor (tarjeta intermedia o LOM) puede tener dos o cuatro puertos, en función de la capacidad. Las ranuras para tarjetas secundarias están ocupadas por las tarjetas de extensión PCIe que están conectados a las tarjetas PCIe (y no a los módulos de E/S). Al implementar las redes Ethernet, iSCSI o FibreChannel, expanda los enlaces redundantes por los tramos uno y dos para obtener la máxima disponibilidad. El módulo de E/S discreto está identificado con un identificador de red Fabric.

NOTA: En la CLI del CMC, al módulo de E/S se lo conoce por la convención "conmutador".

Temas:

- Situación de encendido por primera vez
- Supervisión de la condición del módulo de E/S
- Configuración de los valores de red para módulos de E/S
- Administración de las operaciones de control de alimentación para módulos de E/S
- Activación o desactivación del parpadeo del LED para los módulos de E/S

Situación de encendido por primera vez

Cuando el chasis está conectado y encendido, el módulo de E/S tiene prioridad con respecto a los servidores. Se permite que el módulo de E/S se encienda antes que los demás. En este momento, no se realiza la verificación de sus tipos de red Fabric.

Una vez que se encienden los M. E/S, se encienden los servidores y, a continuación, el CMC verifica la congruencia de red Fabric en los servidores.

Se permite un módulo de paso y un switch en el mismo grupo, siempre y cuando sus redes Fabric sean idénticas. Los switches y módulos de paso pueden existir en el mismo grupo, incluso si fueron fabricados por proveedores distintos.

Supervisión de la condición del módulo de E/S

Para obtener información sobre cómo supervisar la condición del módulo de E/S, consulte Visualización de la información y el estado de condición del M. E/S.

Configuración de los valores de red para módulos de E/S

Puede especificar los valores de red para la interfaz utilizada para administrar el módulo de E/S. Para los switches de Ethernet, se configura el puerto de administración fuera de banda (dirección IP). El puerto de administración en banda (es decir, VLAN1) no se configura mediante esta interfaz.

Antes de configurar los valores de red para los módulos de E/S, asegúrese de que el módulo de E/S esté encendido.

Para configurar los valores de red del módulo de E/S en el grupo A, debe contar con privilegios de administrador de la red Fabric A.

NOTA: En los conmutadores de Ethernet, las direcciones IP de administración en banda (VLAN1) y fuera de banda no pueden ser las mismas ni estar en la misma red. Esto ocasiona que no se configure la dirección IP fuera de banda. Consulte la documentación sobre el módulo de E/S para la dirección IP de administración en banda predeterminada.

NOTA: No intente configurar los valores de la red del módulo de E/S para módulos de paso de Ethernet y conmutadores de Infiniband.

Configuración de los valores de red para los módulos de E/S mediante la interfaz web del CMC

Para configurar los valores de red para los módulos de E/S:

1 En el panel izquierdo, haga clic en **Descripción general del chasis**, haga clic en **Descripción general del módulo de E/S**) y, a continuación, haga clic en **Configuración**. Como alternativa, para configurar los valores de red del único módulo de E/S disponible que es **A**, haga clic en **Ethernet Gigabit A**) y, a continuación, haga clic en **Configuración**.

En la página **Configurar valores de red para los módulos de E/S**, escriba los datos adecuados y haga clic en **Aplicar**.

2 Si está permitido, escriba la contraseña de raíz, la cadena de comunidad de SNMP RO y la dirección IP del servidor Syslog para el módulo de E/S. Para obtener más información sobre las descripciones de los campos, consulte la *Ayuda en línea*.

NOTA: La dirección IP establecida en los módulos de E/S a partir de la CMC no se guarda en la configuración de inicio permanente del conmutador. Para guardar la configuración de la dirección IP en forma permanente, debe ejecutar el comando, `connect switch` o el comando RACADM `racadm connect switch`, o bien, usar una interfaz directa a la interfaz gráfica de usuario del módulo de E/S para guardar esta dirección en el archivo de configuración de inicio.

NOTA: La longitud de la cadena de comunidad SNMP pueden estar en el intervalo de valores de ASCII de 33 a 125 caracteres.

3 Haga clic en **Aplicar**.

Los valores de red se configuran para los módulos de E/S.

NOTA: Si está permitido, es posible restablecer las VLAN, las propiedades de la red y los puertos de E/S a sus valores de configuración predeterminados.

Configuración de los valores de red para los módulos de E/S mediante RACADM

Para configurar los valores de la red para un módulo de E/S mediante RACADM, establezca la fecha y la hora. Consulte la sección del comando en *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Es posible establecer el nombre de usuario, la contraseña y la cadena SNMP para un módulo de E/S mediante el comando deploy de RACADM:

```
racadm deploy -m switch -u <username> -p <password>
```

```
racadm deploy -m switch -u -p <password> -v SNMPv2 <snmpCommunityString> ro
```

```
racadm deploy -a [server|switch] -u <username> -p <password>
```

Administración de las operaciones de control de alimentación para módulos de E/S

Para obtener información para establecer la operación de control de alimentación para módulos de E/S, consulte Executing Power Control Operations on an IOM (Ejecución de las operaciones de control de alimentación en el módulo de E/S).

Activación o desactivación del parpadeo del LED para los módulos de E/S

Para obtener información sobre cómo activar el parpadeo del LED para los módulos de E/S, consulte Configuring LEDs to Identify Components on the Chassis (Configuración de los LED para identificar componentes en el chasis).

14

Administración y supervisión de la alimentación

El chasis PowerEdge FX2/FX2s es el gabinete de servidor modular más eficiente en términos en términos de alimentación. Su diseño permite incluir ventiladores y suministros de energía de alta eficacia y está optimizado para que el aire circule con mayor facilidad por el sistema; además, contiene componentes con alimentación mejorada en todo el gabinete. El diseño de hardware optimizado complementa las sofisticadas capacidades de administración de alimentación integradas en la Chassis Management Controller (CMC), los suministros de energía y el iDRAC para mejorar aún más la eficiencia de alimentación del entorno del servidor.

Las funciones de administración de la alimentación de PowerEdge VRTX permiten a los administradores configurar el gabinete de modo tal que se reduzca el consumo de alimentación y se ajuste la alimentación según lo requiera el entorno específico.

El gabinete modular PowerEdge VRTX consume energía de CA y distribuye la carga por todas las unidades de suministro de energía (PSU) internas. El sistema puede producir hasta 4800 vatios de CA que se asignan a los módulos del servidor y la infraestructura de gabinete asociada. No obstante, esta capacidad puede variar en función de la política de redundancia que seleccione.

El gabinete PowerEdge VRTX se puede configurar para cualquiera de las dos políticas de redundancia que afectan el comportamiento de la unidad de suministro de energía y determinan la manera en la que se notifica a los administradores el estado de redundancia del chasis.

Además, puede controlar la administración de alimentación mediante **OpenManage Power Center (OMPC)**. Cuando OMPC controla la alimentación de manera externa, la CMC todavía mantiene las siguientes funciones:

- Política de redundancia
- Registro remoto de la alimentación
- Conexión dinámica de suministros de energía

El centro OMPC administra, entonces, lo siguiente:

- Alimentación del servidor
- Prioridad de los servidores
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

NOTA: La entrega real de alimentación se basa en la configuración y en la carga de trabajo.

Puede utilizar la interfaz web de la CMC y RACADM para administrar y configurar los controles de alimentación en la CMC:

- Ver las asignaciones, el consumo y el estado de alimentación del chasis, de los servidores y de las unidades de suministro de energía.
- Configurar el presupuesto de alimentación y la política de redundancia del chasis.
- Ejecutar operaciones de control de alimentación (encendido, apagado, restablecimiento del sistema, ciclo de encendido) en el chasis.

Temas:

- Asignación de niveles de prioridad a los servidores mediante la interfaz web del CMC
- Asignación de niveles de prioridad a los servidores mediante RACADM
- Visualización del estado del consumo de alimentación
- Visualización del estado de presupuesto de alimentación mediante la interfaz web del CMC
- Estado de redundancia y condición general de la alimentación
- Configuración de la redundancia y el presupuesto de alimentación
- Ejecución de las operaciones de control de alimentación
- Ejecución de operaciones de control de alimentación en un servidor
- Ejecución de operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC
- Ejecución de operaciones de control de alimentación en el módulo de E/S

Políticas de redundancia

La política de redundancia es un conjunto configurable de propiedades que determina la forma en que la CMC administra la alimentación al chasis. Las siguientes políticas de redundancia son configurables con conexión dinámica de unidad de suministro de energía o sin ella:

- Redundancia de cuadrícula
- Redundancia del suministro de energía

Política de redundancia de la red eléctrica

El objetivo de la política de redundancia de la red eléctrica es permitir que un sistema de gabinete modular funcione de modo que le permita tolerar los errores de alimentación de CA. Es posible que estos errores se originen en la red de corriente alterna, el cableado o el suministro, o bien, en la propia unidad de suministro de energía.

Cuando se configura un sistema para la redundancia de cuadrícula, las unidades de suministro de energía se dividen en cuadrículas: las unidades de las ranuras 1 y 2 se encuentran en la primera cuadrícula, en tanto que las unidades de las ranuras 3 y 4 se encuentran en la segunda cuadrícula. La CMC administra la alimentación de forma tal que si se produce una falla en alguna de las cuadrículas, el sistema seguirá funcionando sin que haya degradación. La redundancia de cuadrícula también tolera las fallas de las unidades de suministro de energía individuales.

NOTA: Dado que una de las funciones de la redundancia de cuadrícula es proporcionar una operación perfecta del servidor a pesar de cualquier falla que se produzca en toda una red eléctrica, la mayor parte de la alimentación se pone a disposición del mantenimiento de la redundancia de cuadrícula cuando las capacidades de las dos redes eléctricas son aproximadamente iguales.

NOTA: La redundancia de cuadrícula solo se cumple cuando los requisitos de carga no superan la capacidad de la red eléctrica más débil.

Niveles de redundancia de la red eléctrica

La configuración mínima necesaria para tener redundancia de cuadrícula es tener una unidad de suministro de energía en cada cuadrícula. Es posible definir configuraciones adicionales con cada combinación que contenga al menos una unidad de suministro de energía en cada cuadrícula. Sin embargo, para poder usar el máximo nivel de energía, la energía total de las unidades de suministro de energía de cada cuadrícula debe ser lo más similar posible. El límite máximo de energía mientras se mantiene la redundancia de cuadrícula es la energía disponible en la cuadrícula más débil.

Si el CMC no puede mantener la redundancia de cuadrícula, se envían alertas de correo electrónico y/o SNMP a los administradores, siempre que el suceso Redundancia perdida esté configurado para el envío de alertas.

Si una sola unidad de suministro de energía no funciona en esta configuración, las unidades de suministro de energía restantes en la cuadrícula que causa el problema se marcan como en línea. En este estado, las unidades de suministro de energía de la cuadrícula redundante, si no están en estado de falla, ayudan en el funcionamiento del sistema sin interrupción. Si una unidad de suministro de energía deja de funcionar, la condición del chasis se identifica como no crítica. Si la cuadrícula más pequeña no puede admitir las asignaciones

totales de energía del chasis, se informa el estado de redundancia de la cuadrícula como **No** y la condición del chasis se muestra como **Crítica**.

Política de redundancia de suministro de energía

La política de redundancia de suministro de energía es útil cuando las redes de energía redundante no están disponibles, pero es posible que desee estar protegido contra una falla de una única unidad de suministro de energía que deje fuera de servicio a los servidores en un gabinete modular. La unidad de suministro de energía de mayor capacidad se mantiene en reserva en línea para este propósito. Esto forma un grupo de redundancia de suministro de energía.

Las demás unidades de suministro de energía además de las necesarias para alimentación y redundancia siguen disponibles y se agregan al grupo en caso de falla.

A diferencia de la redundancia de cuadrícula, cuando se selecciona la redundancia de suministro de energía, el CMC no requiere que las unidades de suministro de energía estén presentes en ninguna posición específica de las ranuras de las unidades de suministro de energía.

NOTA: La conexión dinámica del suministro de energía (DPSE) permite poner en espera las unidades de suministro de energía. El estado en espera indica una estado físico de las unidades de suministro de energía en el que no se suministra alimentación. Al activar DPSE, las unidades de suministro de energía adicionales pueden ponerse en modo de espera para aumentar la eficiencia y ahorrar energía.

NOTA: Modifique la política de redundancia del gabinete modular mientras el gabinete está apagado.

Conexión dinámica de suministros de energía

De forma predeterminada, el modo de Conexión dinámica de suministros de energía (DPSE) está desactivado. DPSE ahorra energía al optimizar la eficiencia energética de las unidades de suministro de energía que suministran energía al chasis. Esto también aumenta la vida útil de las unidades de suministro de energía y evita que se genere demasiado calor. Para usar esta función, debe tener una licencia Enterprise.

La CMC supervisa la asignación de alimentación total al gabinete y coloca las unidades de suministro de energía en estado En espera, lo que provoca que la asignación de alimentación total del chasis se realice a través de menos unidades de suministro de energía. Debido a que las unidades de suministro de energía en línea son más eficientes cuando funcionan con niveles más altos de uso, esto mejora su eficiencia y la longevidad de las unidades de suministro de energía en espera.

Para operar las unidades de suministro de energía restantes en su máxima eficiencia, use los siguientes modos de redundancia de alimentación:

- El modo de **Redundancia de las unidades de suministro energía** con DPSE proporciona eficiencia energética. Al menos dos suministros se encuentran en línea, con una unidad de suministro de energía requerida para alimentar la configuración y otra para proporcionar redundancia en caso de falla de la unidad de suministro de energía. El modo de Redundancia de las unidades de suministro de energía ofrece protección contra la falla de cualquier unidad de suministro de energía, pero no ofrece protección en caso de una pérdida de la red eléctrica de CA.
- Modo **Redundancia de cuadrícula** con DPSE, en donde por lo menos dos unidades de suministro de energía están activas, una en cada red eléctrica. La redundancia de cuadrícula equilibra también la eficiencia y la disponibilidad máxima para una configuración de gabinete modular parcialmente cargado.
- La desactivación de DPSE proporciona la más baja eficiencia ya que las cuatro fuentes están activas y comparten la carga, lo cual produce una utilización más baja de cada suministro de energía.

La DPSE puede activarse para las dos configuraciones de redundancia de suministro de energía explicadas anteriormente: **Redundancia de suministro de energía** y **Redundancia de cuadrícula**.

NOTA: En los modos de una configuración de dos unidades de suministro de energía, la carga del servidor puede evitar que cualquier unidad de suministro de energía cambie al modo En espera.

- En una configuración de **Redundancia del suministro de energía**, además de las unidades de suministro de energía requeridas para alimentar el gabinete, este siempre mantiene una unidad de suministro de energía adicional encendida y marcada como **En línea**. Se supervisa el uso de energía y una unidad de suministro de energía se puede colocar en estado En espera en función de la carga total del

sistema. En una configuración de cuatro unidades de suministro de energía, siempre están encendidas un mínimo de dos unidades de suministro de energía.

Debido a que un gabinete en la configuración **Redundancia del suministro de energía** siempre tiene una unidad de suministro de energía adicional conectada, el gabinete puede adecuar la pérdida de una unidad de suministro de energía en línea y aún tener suficiente energía para los módulos de servidor instalados. La pérdida de la unidad de suministro de energía en línea hará que una unidad en espera pase a estar en línea. La falla simultánea de varias unidades de suministro de energía puede ocasionar la pérdida de corriente en algunos módulos de servidor mientras que las unidades de suministro de energía en espera se encienden.

- En la configuración **Redundancia de cuadrícula**, todas las unidades de suministro de energía están conectadas al encenderse el chasis. Se supervisa el uso de energía y, si lo permiten la configuración del sistema y la utilización de energía, las unidades de suministro de energía se trasladan al estado **En espera**. Debido a que el estado **En línea** de las unidades de suministro de energía en una red eléctrica refleja el modo de la otra red eléctrica, el gabinete puede soportar la pérdida de alimentación de una red eléctrica entera sin interrumpir la alimentación al gabinete.

  Un aumento de la demanda de energía en la configuración de la **Redundancia de la cuadrícula** hará que las unidades de suministro de energía se activen y salgan del estado **En espera**. Esto mantiene la configuración duplicada necesaria para la redundancia de doble cuadrícula.

NOTA: Con DPSE en estado activado, si la demanda de energía aumenta en los dos modos de políticas de redundancia de alimentación, las unidades de suministro de energía en espera se colocan En línea para recuperar energía.

Configuración predeterminada de redundancia

Como se muestra en la tabla a continuación, la configuración predeterminada de redundancia de un chasis depende del número de unidades de suministro de energía que contiene.

Tabla 37. Configuración predeterminada de redundancia

Configuración de unidades de suministro de energía	Política de redundancia predeterminada	Valor predeterminado de la conexión dinámica de unidades de suministro de energía
Dos unidades de suministro de energía	Redundancia de CC	Desactivado
Cuatro unidades de suministro de energía	Redundancia de CC	Desactivado

Redundancia de cuadrícula

En el modo de redundancia de cuadrícula con cuatro unidades de suministro de energía, las cuatro unidades están activas. Las dos unidades deben conectarse a una red eléctrica de alimentación de CA, en tanto que las otras dos unidades se conectan a la otra red eléctrica de alimentación de CA.

PRECAUCIÓN: Para evitar una falla del sistema y para que la redundancia de cuadrícula funcione de manera eficaz, debe haber un conjunto equilibrado de unidades de suministro de energía correctamente cableadas a redes de CA independientes.

Si una red de CA falla, las unidades de suministro de energía de la red de CA en funcionamiento tomarán el control sin que se interrumpan los servidores o la infraestructura.

PRECAUCIÓN: En el modo de redundancia de cuadrícula, debe tener conjuntos equilibrados de unidades de suministro de energía (al menos una unidad en cada red eléctrica). Si esta condición no se cumple, la redundancia de cuadrícula no será posible.

Redundancia del suministro de energía

Cuando se activa la redundancia de suministro de energía, una de las unidades de suministro de energía del chasis se mantiene como repuesto, lo cual garantiza que la falla de una de las unidades no ocasione que se apaguen los servidores o el chasis. El modo de

redundancia de suministro de energía requiere un mínimo de dos unidades de suministro de energía. Si existen unidades de suministro de energía adicionales, serán utilizadas para mejorar la eficiencia energética del sistema cuando la DPSE esté activada. Las fallas posteriores a una pérdida de redundancia pueden provocar que los servidores del chasis se apaguen.

Presupuesto de alimentación para módulos de hardware

El CMC ofrece un servicio de presupuesto de alimentación que le permite configurar el presupuesto de alimentación, la redundancia y la alimentación dinámica para el chasis.

El servicio de administración de la alimentación permite optimizar el consumo de alimentación y reasignar la alimentación a diferentes módulos en función de la demanda.

El CMC mantiene un presupuesto de alimentación para el gabinete que reserva la potencia necesaria para todos los servidores y componentes instalados.

La CMC asigna alimentación a la infraestructura de la CMC y los servidores en el chasis. La infraestructura de la CMC consta de componentes en el chasis, como ventiladores, módulo de E/S y adaptadores de almacenamiento, tarjetas PCIe, disco físico y placa principal. El chasis puede tener hasta cuatro servidores que se comunican con este a través de un iDRAC. Para obtener más información, consulte *iDRAC User's Guide* (Guía del usuario de iDRAC) en **dell.com/support/manuals**.

El iDRAC presenta a la CMC los requisitos de la envolvente de potencia antes de brindar alimentación al servidor. La envolvente de potencia consiste en los requisitos de alimentación máxima y mínima necesarios para mantener el servidor en funcionamiento. El cálculo inicial del iDRAC se basa en la comprensión inicial de los componentes en el servidor. Después de iniciar el funcionamiento y descubrir otros componentes, el iDRAC puede aumentar o reducir sus requisitos de alimentación iniciales.

Cuando se enciende un servidor en un gabinete, el software del iDRAC vuelve a calcular los requisitos de alimentación y solicita el cambio correspondiente en la envolvente de potencia.

La CMC suministra la alimentación solicitada al servidor y la potencia asignada se resta del presupuesto disponible. Una vez que se otorga una solicitud de alimentación al servidor, el software del iDRAC del servidor supervisa continuamente el consumo de alimentación real. En función de los requisitos de alimentación real, la envolvente de potencia del iDRAC puede cambiar al cabo de un período de tiempo. iDRAC solicita un aumento de alimentación si los servidores utilizan en forma total la alimentación asignada.

En condiciones de carga pesada, el funcionamiento de los procesadores del servidor puede degradarse para garantizar que el consumo de alimentación se mantenga por debajo del valor de Límite de alimentación de entrada del sistema configurado por el usuario.

El gabinete PowerEdge VRTX puede suministrar alimentación suficiente para un rendimiento máximo de la mayoría de las configuraciones de servidores, pero varias configuraciones de servidores disponibles no consumen la alimentación máxima que el gabinete puede suministrar. Para ayudar a los centros de datos a asignar alimentación a sus gabinetes, PowerEdge VRTX le permite especificar un Límite de alimentación de entrada del sistema para garantizar que la alimentación de CA general del chasis permanezca dentro de un punto umbral dado. La CMC garantiza primero que haya suficiente alimentación disponible para hacer funcionar los ventiladores, el módulo de E/S, los adaptadores de almacenamiento, las unidades de discos físicos, la placa principal y la propia CMC. Esta asignación de energía se denomina Energía de entrada asignada a la infraestructura del chasis. Después de la infraestructura del chasis, se encienden los servidores en un gabinete. Cualquier intento de establecer un Límite de alimentación de entrada del sistema menor a la "carga de alimentación" no tendrá éxito. La carga de alimentación es la suma de alimentación asignada a la infraestructura y la alimentación mínima asignada a los servidores conectados.

NOTA: Para usar la función de límite de energía, el usuario debe tener una licencia Enterprise.

Si se debe mantener el presupuesto total de alimentación por debajo del valor del *Límite de alimentación de entrada del sistema*, la CMC asigna a los servidores un valor menor que la alimentación máxima solicitada. A los servidores se les asigna alimentación en base a la configuración de *Prioridad del Servidor*, en donde los servidores con mayor prioridad reciben el máximo de alimentación, los servidores con prioridad 2 reciben alimentación después de los servidores con prioridad 1, y así sucesivamente. Los servidores con menor prioridad pueden

recibir menos alimentación que los servidores de prioridad 1, de acuerdo a la *Capacidad máxima de alimentación de entrada del sistema*, y el valor configurado por el usuario del*Límite de alimentación de entrada del sistema*.

Los cambios de configuración, como un servidor adicional, HDD compartidos o tarjetas PCIe en el chasis, pueden requerir el aumento del *Límite de alimentación de entrada del sistema*. Las necesidades energéticas en un gabinete modular aumentan también cuando cambian las condiciones térmicas y los ventiladores deben funcionar a mayor velocidad, lo que hace que consuman energía adicional. La colocación de módulos de E/S y adaptadores de almacenamiento, tarjetas PCIe, disco físico, placa principal, número, tipo y configuración de PSU también aumentan las necesidades energéticas del gabinete modular. Aunque estén apagados, los servidores consumen una pequeña cantidad de energía para mantener a la controladora de administración encendida.

Los servidores adicionales se pueden encender en el gabinete modular solamente si hay suficiente energía disponible. El *Límite de alimentación de entrada del sistema* puede aumentarse en cualquier momento hasta un valor máximo de 5000 vatios para permitir el encendido de servidores adicionales.

Los cambios en el gabinete modular que reducen la asignación de alimentación son:

- El servidor se apagó
- El módulo de E/S se apagó
- Los adaptadores de almacenamiento, las tarjetas PCIe, la unidad de disco físico y la placa principal se apagaron
- Transición del chasis al estado apagado

Los usuarios pueden reconfigurar el *Límite de alimentación de entrada del sistema* cuando el chasis está encendido o apagado.

Configuración de la prioridad de alimentación de ranura del servidor

La CMC le permite establecer una prioridad de alimentación para cada una de las cuatro ranuras de servidores de un gabinete. Los valores de prioridad son de 1 (la más alta) a 9 (la más baja). Estos valores se asignan a ranuras del chasis y la prioridad de las ranuras es heredada por cualquier servidor insertado en esa ranura. La CMC utiliza la prioridad de la ranura para administrar alimentación de manera preferencial a los servidores de más alta prioridad en el gabinete.

Según el valor predeterminado de prioridad de ranura del servidor, la alimentación se distribuye por igual a todas las ranuras. El cambio de prioridades de ranura permite a los administradores priorizar los servidores a los que se dará preferencia de asignaciones de alimentación. Si los módulos de servidor más críticos se dejan con la prioridad de ranura predeterminada de 1 y los módulos de servidor menos críticos se cambian al valor de prioridad más bajo de 2, los módulos de servidor de prioridad 1 se encienden primero. Estos servidores de prioridad más alta obtienen su asignación de alimentación máxima, mientras que a los servidores de prioridad más baja puede que no se les asigne suficiente alimentación para funcionar a su máximo rendimiento o puede que no se los encienda en absoluto, dependiendo de cuán bajo se establece el límite de alimentación de entrada del sistema y los requisitos de alimentación del servidor.

Si un administrador enciende manualmente los módulos del servidor de baja prioridad antes que los de prioridad más alta, los módulos del servidor de prioridad baja serán los primeros módulos a los que se les disminuirá la asignación de alimentación a su valor mínimo, a fin de abastecer a los servidores de mayor prioridad. Por lo tanto, cuando se agota la alimentación disponible para asignación, la CMC retira alimentación de los servidores de prioridad inferior o igual hasta que alcancen el nivel mínimo de alimentación.

NOTA: El módulo de E/S, los ventiladores, la placa principal, las unidades de disco físico y los adaptadores de almacenamiento reciben la mayor prioridad. La CMC retira alimentación únicamente de los dispositivos de prioridad más baja para satisfacer las necesidades de alimentación de un servidor o dispositivo de prioridad más alta.

Asignación de niveles de prioridad a los servidores

Cuando se requiere alimentación adicional, los niveles de prioridad de los servidores determinan los servidores desde donde el CMC extrae energía.

NOTA: La prioridad que se asigna a un servidor está vinculada a la ranura del servidor y no al propio servidor. Si traslada el servidor a una nueva ranura, debe reconfigurar la prioridad para la ubicación de la nueva ranura.

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de Administrador de configuración del chasis.

Asignación de niveles de prioridad a los servidores mediante la interfaz web del CMC

Para asignar niveles de prioridad:

1 En el panel izquierdo, haga clic en **Descripción general del servidor** > **Alimentación** > **Prioridad**.
La página **Prioridad de los servidores** muestra todos los servidores del chasis.

2 Desde el menú desplegable **Prioridad**, seleccione un nivel de prioridad (de 1 a 9, siendo 1 la prioridad máxima) para uno, varios o todos los servidores. El valor predeterminado es 1. Puede asignar el mismo nivel de prioridad para varios servidores.

3 Haga clic en **Apply (Aplicar)** para guardar los cambios.

Asignación de niveles de prioridad a los servidores mediante RACADM

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

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <slot number> <priority level>
```

donde *<slot number>* (de 1 a 4) se refiere a la ubicación del servidor y *<priority level>* es un valor entre 1 y 9.

Por ejemplo, para establecer el nivel de prioridad en 1 para el servidor en la ranura 4, escriba el siguiente comando:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 4 1
```

Visualización del estado del consumo de alimentación

La CMC proporciona el consumo real de alimentación de entrada para todo el sistema.

Visualización del estado del consumo de alimentación mediante la interfaz web del CMC

En el panel izquierdo, haga clic en **Descripción general del chasis.** > **Alimentación** > **Supervisión de alimentación**. La página Supervisión de alimentación muestra la condición de la alimentación, el estado de la alimentación del sistema, y estadísticas de alimentación y de energía en tiempo real. Para obtener más información, consulte la *Ayuda en línea*.

NOTA: También puede ver el estado de redundancia de alimentación en la opción Suministros de energía.

Visualización del estado del consumo de alimentación con el comando RACADM

Para ver el estado del consumo de alimentación con el comando RACADM:

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

```
racadm getpminfo
```

AC Power Recovery

Si la fuente de alimentación de CA de un sistema se interrumpe, el chasis se restaura al estado de energía previo a la pérdida de alimentación de CA. La restauración al estado anterior de la alimentación es el comportamiento predeterminado. Los siguientes factores podrían ocasionar la interrupción:

- interrupción de la alimentación
- cables de alimentación extraídos de las unidades de suministro de energía (PSU)
- interrupciones en las unidades de distribución de alimentación (PDU)

Si la opción **Configuración de redundancia/presupuesto** > **Desactivar recuperación de alimentación de CA** está seleccionada, el chasis permanece apagado después de la recuperación de la CA.

En este caso, los servidores blade no están configurados para el encendido automático, y es posible que tenga que encenderlos manualmente.

Visualización del estado de presupuesto de alimentación mediante la interfaz web del CMC

Para ver el estado de presupuesto de alimentación mediante la interfaz web de la CMC, en el panel izquierdo, vaya a **Descripción general del chasis** y, a continuación, haga clic en **Alimentación** > **Estado de presupuesto**. La página **Estado de presupuesto de alimentación** muestra la configuración de la política de alimentación del sistema, los detalles del presupuesto de alimentación, el presupuesto asignado para los módulos del servidor y los detalles del suministro de energía del chasis. Para obtener más información, consulte la *Ayuda en línea*.

Visualización del estado del presupuesto de alimentación mediante RACADM

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

```
racadm getpbinfo
```

Para obtener más información sobre **getpbinfo**, incluidos los detalles de salida, consulte la sección del comando **getpbinfo** en la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia sobre la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Estado de redundancia y condición general de la alimentación

El estado de redundancia es un factor determinante de la condición general de la alimentación. Cuando se establece la política de redundancia de alimentación, por ejemplo, en Redundancia de cuadrícula, y el estado de redundancia indica que el sistema funciona con redundancia, la condición general de la alimentación normalmente será **En buen estado**. Si la unidad de suministro de energía instalada en un chasis falla por alguna razón, el estado de la condición general de la alimentación del chasis se muestra como **No crítico**. Sin embargo, si no se satisfacen las condiciones para operar con redundancia de cuadrícula, el estado de redundancia será **No,** y la condición general de la alimentación será **Crítica**. Esto se debe a que el sistema no puede funcionar de acuerdo con la política de redundancia configurada.

NOTA: La CMC no realiza una comprobación previa de estas condiciones cuando la política de redundancia se cambia a Redundancia de la cuadrícula o de esta última a otra. Por lo tanto, configurar la política de redundancia podría ocasionar inmediatamente una pérdida de redundancia o una condición de recuperación.

Administración de la alimentación tras un error de la unidad de suministro de energía

Cuando se produce un suceso de falta de alimentación, como por ejemplo, una falla en una unidad de suministro de energía, la CMC reduce el suministro de energía a los servidores. Una vez reducido el suministro, la CMC reevalúa las necesidades de alimentación del chasis. Si aún no se cumplen los requisitos, la CMC apaga los servidores de menor prioridad. No obstante, esto se hace en función de la política de redundancia de alimentación que haya establecido en la CMC. Un servidor redundante puede tolerar la pérdida de alimentación sin que se afecte el rendimiento de los servidores.

La alimentación a los servidores de mayor prioridad se restablece gradualmente, en tanto que las necesidades de alimentación se ajustan al presupuesto de alimentación. Para establecer la política de redundancia, consulte Configuración de la redundancia y el presupuesto de alimentación.

Administración de la alimentación tras la desconexión de una unidad de suministro de energía

Es posible que la CMC comience a conservar energía cuando se quita una unidad de suministro de energía o se quita el cable de CA de la misma. La CMC reduce la alimentación de los servidores con menor prioridad hasta que la asignación de energía esté cubierta por las unidades de suministro de energía restantes en el chasis. Si quita más de una unidad de suministro de energía, la CMC volverá a evaluar los requisitos de alimentación al quitar la segunda unidad de suministro de energía a fin de determinar la respuesta del firmware. Si aún no se cumplen los requisitos de alimentación, es posible que la CMC apague los servidores de menor prioridad.

Límites

- El CMC no admite el apagado *automatizado* de un servidor con menor prioridad para permitir el encendido de un servidor con mayor prioridad; sin embargo, se pueden realizar apagados iniciados por el usuario.
- Los cambios en la política de redundancia de las unidades de suministro de energía están limitados por el número de unidades de suministro de energía en el chasis. Se puede seleccionar cualquiera de los dos valores de configuración de la redundancia de las unidades de suministro de energía que se enumeran en la Configuración predeterminada de redundancia.

Política de conexión de servidores nuevos

Si un servidor nuevo que está encendido supera la alimentación disponible para el chasis, es posible que la CMC disminuya la alimentación hacia los servidores de menor prioridad. Esto podría suceder si el administrador ha configurado un límite de alimentación para el chasis que está por debajo de lo requerido para la asignación de toda la alimentación a los servidores, o si hay alimentación insuficiente en caso de requisitos de mayor alimentación por todos los servidores en el chasis. Si no se puede liberar suficiente alimentación mediante la reducción de la alimentación asignada a los servidores con menor prioridad, el nuevo servidor no se puede encender.

Esto ocurre si el administrador había configurado un límite de alimentación para el chasis inferior a la asignación de alimentación total a los servidores o si la alimentación insuficiente está disponible para los servidores que requieren mayor alimentación.

En la siguiente tabla se describen las acciones realizadas por el CMC cuando se enciende un nuevo servidor en las condiciones descritas anteriormente.

Tabla 38. Respuesta del CMC cuando se intenta encender un servidor

Se cuenta con alimentación para el peor de los casos	Respuesta del CMC	Encendido del servidor
Sí	No se requiere la conservación de energía	Permitido
No	Se ejecuta la conservación de energía:	Permitido
	• La alimentación requerida para el nuevo servidor está disponible	No permitido
	• La alimentación requerida para el nuevo servidor no está disponible	

Si una unidad de suministro de energía deja de funcionar, se produce un estado no crítico y se genera un suceso de falla de unidad de suministro de energía. Al desmontar una unidad de suministro de energía se genera un suceso de desmontaje de una unidad de suministro de energía.

Si uno de los sucesos ocasiona una pérdida de redundancia, en función de las asignaciones de alimentación, se genera un suceso de *pérdida de redundancia*.

Si la capacidad de alimentación posterior o la capacidad de alimentación del usuario es mayor que las asignaciones de los servidores, el rendimiento de los servidores se verá degradado o, en el peor de los casos, los servidores pueden llegar a apagarse. Ambas condiciones se dan en orden de prioridad inverso, es decir, los servidores de menor prioridad se apagan primero.

En la siguiente tabla se describe la respuesta del firmware ante el apagado o el desmontaje de una unidad de suministro de energía conforme se aplica a diversas configuraciones de redundancia de las unidades de suministro de energía.

Tabla 39. Impacto en el chasis de la falla o el desmontaje de una unidad de suministro de energía

Configuración de unidades de suministro de energía	Acoplamiento dinámico de unidades de suministro de energía	Respuesta del firmware
Redundancia de cuadrícula	Desactivado	El CMC envía alertas acerca de la pérdida de redundancia de cuadrícula.
Redundancia del suministro de energía	Desactivado	El CMC envía alertas acerca de la pérdida de redundancia del suministro de alimentación.
Redundancia de cuadrícula	Activado	La CMC lo alerta de la pérdida de redundancia de cuadrícula. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el desmontaje de una unidad de suministro de energía.
Redundancia del suministro de energía	Activado	El CMC informa al usuario que hay pérdida de redundancia de suministro de energía. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el desmontaje de una unidad de suministro de energía.

Cambios de suministro de energía y política de redundancia en el registro de sucesos del sistema

Los cambios en el estado de suministro de energía y en la política de redundancia de la alimentación se registran como sucesos. Los sucesos relacionados con el suministro de energía que registran anotaciones en el registro de sucesos del sistema (SEL) son inserción y extracción

de suministros de energía, inserción y extracción de entrada de suministros de energía, y declaración y retiro de declaración de salida de suministros de energía.

La siguiente tabla incluye las anotaciones en el SEL que están relacionadas con los cambios en el suministro de energía:

Tabla 40. Sucesos del SEL para cambios de suministros de energía

Suceso de suministro de energía	Anotación del registro de sucesos del sistema (SEL)
Inserción	Hay suministro de energía.
Extracción	Falta el suministro de energía.
Entrada de CA recibida	Se ha restablecido la entrada de corriente del suministro de energía.
Entrada de CA perdida	Se ha perdido la entrada de corriente del suministro de energía <número>.
Salida de CC producida	El suministro de energía funciona normalmente.
Salida de CC perdida	Falló el suministro de energía.

Los sucesos relacionados con cambios en el estado de redundancia de alimentación que registran anotaciones en el SEL son la pérdida de redundancia y la recuperación de redundancia para el gabinete modular que está configurado para una política de alimentación de **Redundancia de cuadrícula** o para una política de **Redundancia de alimentación.** En la tabla siguiente se enumeran las anotaciones del SEL relacionadas con los cambios en la política de redundancia de alimentación.

Tabla 41. Sucesos del SEL para cambios en la política de redundancia de alimentación

Suceso de política de alimentación	Anotación del registro de sucesos del sistema (SEL)
Redundancia perdida	Se ha perdido la redundancia de la fuente de alimentación.
Redundancia recuperada	The power supplies are redundant. (Las fuentes de alimentación son redundantes).

Configuración de la redundancia y el presupuesto de alimentación

Puede configurar el presupuesto de alimentación, la redundancia y la alimentación dinámica de todo el chasis (chasis, servidores, módulo de E/S, KVM, CMC y suministros de energía), el cual utiliza cuatro unidades de suministro de energía (PSU). El servicio de administración de alimentación optimiza el consumo de energía y reasigna la alimentación eléctrica a los distintos módulos en función de los requisitos.

Puede configurar los siguientes atributos:

- Límite de alimentación de entrada del sistema
- Política de redundancia
- Activar conexión dinámica del suministro de energía
- Desactivar botón de encendido del chasis
- Modo de conservación máx. de alimentación
- Registro remoto de la alimentación
- Intervalo del registro remoto de la alimentación
- Administración de la alimentación basada en servidor
- Desactivar restablecimiento de la alimentación de CA

Conservación de la energía y presupuesto de alimentación

La CMC conserva la alimentación cuando se llega al límite de alimentación máxima configurado por el usuario. Cuando la demanda de energía supera el límite de alimentación de entrada del sistema configurado por el usuario, la CMC reduce la alimentación a los servidores en orden de prioridad inverso para liberar energía y enviarla a los servidores de mayor prioridad y otros módulos del chasis.

Si todas o varias ranuras del chasis están configuradas con el mismo nivel de prioridad, la CMC disminuye la alimentación a los servidores a medida que aumenta el número de ranuras. Por ejemplo, si los servidores en las ranuras 1 y 2 tienen el mismo nivel de prioridad, la alimentación para el servidor en la ranura 1 se reduce antes que la del servidor en la ranura 2.

NOTA: Puede asignar un nivel de prioridad a cada uno de los servidores en el chasis asignándole un número del 1 al 9 a cada uno. El nivel de prioridad predeterminada para todos los servidores es 1. Cuanto menor es el número, mayor es el nivel de prioridad.

El presupuesto de alimentación se limita al máximo del grupo de dos unidades de suministro de energía que sea el más débil. Si intenta establecer un valor de presupuesto de alimentación de CA que exceda el valor *límite de alimentación de entrada del sistema*, la CMC mostrará un mensaje. El presupuesto de alimentación se limita a 4800 vatios.

Modo de conservación máxima de energía

Esto se activa para los modos Redundancia de cuadrícula o Redundancia de unidad de suministro de energía. El CMC realiza una conservación máxima de energía en los siguientes casos:

- El modo de conservación máxima está activado.
- Una secuencia de línea de comandos automatizada emitida por una fuente de alimentación ininterrumpible activa el modo de conservación máxima.

En el modo de conservación máxima de energía, todos los servidores comienzan a funcionar a su nivel mínimo de energía y todas las solicitudes posteriores de asignación de energía del servidor se rechazan. En este modo, el rendimiento de los servidores encendidos puede degradarse. Los servidores adicionales no pueden encenderse, independientemente de la prioridad del servidor.

El sistema se restablece al rendimiento óptimo cuando se desactiva el modo de conservación máxima.

NOTA: Si el Modo de conservación de máxima alimentación (MPCM) se encuentra activado en el chasis, todas las solicitudes de alimentación de un servidor blade se rechazan. El servidor blade no se enciende si no hay ninguna acción en el iDRAC o el servidor blade que requieran que el host inicie el ciclo de encendido.

Reducción de la alimentación del servidor para mantener el presupuesto de alimentación

La CMC reduce las asignaciones de alimentación a los servidores de menor prioridad cuando se necesita energía adicional para mantener el consumo de alimentación del sistema dentro del *Límite de alimentación de entrada del sistema* configurado por el usuario. Por ejemplo, cuando se conecta un nuevo servidor, la CMC podría reducir la alimentación a los servidores de menor prioridad para obtener más alimentación para el servidor nuevo. Si después de reducir las asignaciones de alimentación a los servidores de menor prioridad, la energía aún no es suficiente, la CMC disminuirá el rendimiento de los servidores hasta liberar suficiente energía para alimentar el servidor nuevo.

El CMC reduce la asignación de alimentación a los servidores en dos casos:

- El consumo general de alimentación excede el valor de *Límite de alimentación de entrada del sistema*.
- Se produce una falla de alimentación en una configuración sin redundancia.

Operación de unidades de suministro de energía de 110 V

De manera predeterminada, la función de operación de CA de la unidad de suministro de energía a 110 V está disponible. Sin embargo, no se admite una combinación de operación a 110 V y 220 V. Si la CMC detecta que ambos voltajes son de entrada, se selecciona un valor de voltaje y se desactivan esos suministros de energía conectados al otro nivel de voltaje y se indican como fuera de funcionamiento.

Registro remoto

Se puede informar sobre el consumo de alimentación a un servidor syslog remoto. Se puede registrar información sobre el consumo de alimentación total del chasis, como del consumo de alimentación mínimo, máximo y promedio en un período de recopilación. Para obtener más información sobre la manera de activar esta función y configurar el intervalo de recopilación o registro, consulte Administración y supervisión de la alimentación.

Administración de la alimentación externa

La administración de la alimentación de la CMC se controla opcionalmente mediante OpenManage Power Center (OMPC). Para obtener más información, consulte la *Guía del usuario del iDRAC*.

Si está activada la administración de la alimentación externa, OMPC administra lo siguiente:

- Alimentación de servidores VRTX compatibles
- Alimentación de servidores VRTX compatibles
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

El CMC sigue manteniendo o administrando lo siguiente:

- Política de redundancia
- Registro remoto de la alimentación
- Rendimiento del sistema sobre redundancia de alimentación
- Conexión dinámica de suministros de energía

Luego, OMPC administra la priorización y la alimentación de los nodos de servidores VRTX admitidos en el chasis con el presupuesto disponible tras la asignación de alimentación a la infraestructura de chasis y los nodos de servidores de generaciones anteriores. El registro remoto de la alimentación no se ve afectado por la administración de la alimentación externa.

Una vez que se haya activado el Modo de administración de la alimentación basada en servidor, el chasis estará preparado para la administración de la PM3. Todas las prioridades del servidor VRTX compatibles se establecen en 1 (Alta). La PM3 administra las prioridades y la alimentación de los servidores en forma directa. Debido a que la PM3 controla las asignaciones de alimentación del servidor compatible, la CMC ya no controla el Modo de conservación máxima de energía Por ende, esta selección queda desactivada.

Cuando el **Modo de conservación máxima de alimentación** está activado, la CMC establece la capacidad de alimentación de entrada del sistema en el máximo que admite el chasis. La CMC no permite que la alimentación supere la capacidad máxima. Sin embargo, la PM3 administra todos los demás límites de capacidad de alimentación.

Si la administración de la alimentación de la PM3 está desactivada, el CMC vuelve a los valores de prioridad de los servidores configurados antes de que se activase la administración externa.

NOTA: Cuando la administración de la PM3 está desactivada, la CMC no vuelve a la configuración anterior de la alimentación máxima del chasis. Consulte el registro de la CMC para que la configuración anterior restaure el valor manualmente.

Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web del CMC

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de Administrador de configuración del chasis.

Para configurar el presupuesto de alimentación:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Alimentación** > **Configuración**.

2 En la página **Configuración de redundancia/presupuesto**, seleccione alguna o todas las siguientes propiedades según corresponda. Para obtener más información sobre las descripciones de los campos, consulte la *Ayuda en línea*.

- **Activar administración de la alimentación basada en servidor**
- **Límite de alimentación de entrada del sistema**
- **Política de redundancia**
- **Activar conexión dinámica del suministro de energía**
- **Desactivar botón de encendido del chasis**
- **Modo de conservación máx. de alimentación**
- **Activar registro de alimentación remoto**
- **Intervalo del registro remoto de la alimentación**

3 Haga clic en **Aplicar** para guardar los cambios.

Configuración de la redundancia y el presupuesto de alimentación mediante RACADM

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de Administrador de configuración del chasis.

Para activar la redundancia y establecer la política de redundancia:

1 Abra una consola de texto de serie/Telnet/SSH en la CMC e inicie sesión.

2 Establezca las propiedades según sea necesario:

- Para seleccionar una política de redundancia, escriba:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisRedundancyPolicy <value>
  ```

  donde <*value*> es 1 (Redundancia de cuadrícula) y 2 (Redundancia de suministro de energía). El valor predeterminado es 2.

  Por ejemplo, el siguiente comando establece la política de redundancia en 1:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisRedundancyPolicy 1
  ```

- Para establecer el valor del presupuesto de alimentación, escriba:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisPowerCap <value>
  ```

  donde <*valor*> es un número entre 938 W y 4800 W, que representa el límite máximo de la alimentación en vatios. El valor predeterminado es 4800.

  Por ejemplo, el siguiente comando establece el presupuesto máximo de la alimentación en 4800 vatios:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisPowerCap 4800
  ```

- Para activar o desactivar la conexión dinámica de las unidades de suministro de energía, escriba:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisDynamicPSUEngagementEnable <value>
  ```

  donde <*valor*> es 0 (desactivar), 1 (activar). El valor predeterminado es 0.

  Por ejemplo, el siguiente comando desactiva el acoplamiento dinámico de unidades de suministro de energía:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisDynamicPSUEngagementEnable 0
  ```

- Para activar el modo de consumo máximo de alimentación, escriba:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisMaxPowerConservationMode 1
  ```

- Para restaurar el funcionamiento normal, escriba:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisMaxPowerConservationMode 0
  ```

- Para activar la función de registro remoto de alimentación, introduzca el comando siguiente:

  ```
  racadm config -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingEnabled 1
  ```

- Para especificar el intervalo de registro deseado, introduzca el comando siguiente:

  ```
  racadm config -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingInterval n
  ```

  donde *n* es un valor de 1 a 1.440 minutos.

- Para comprobar que la función de registro remoto de alimentación está activada, introduzca el comando siguiente:

  ```
  racadm getconfig -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingEnabled
  ```

- Para determinar el intervalo de registro remoto de alimentación, escriba el comando siguiente:

  ```
  racadm getconfig -g cfgRemoteHosts -o
  cfgRhostsSyslogPowerLoggingInterval
  ```

  La función de registro remoto de alimentación depende de que los hosts de syslog remoto se hayan configurado previamente. El registro en uno o más hosts de syslog remoto debe estar activado; en caso contrario, se registrará el consumo de energía. Esto se puede realizar mediante la interfaz gráfica de usuario web o la CLI de RACADM. Para obtener más información, consulte las instrucciones de configuración de syslog remoto.

- Para activar la administración de alimentación remota por Open Manage Power Center (OPMC), escriba:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisServerBasedPowerMgmtMode 1
  ```

- Para restaurar la administración de la alimentación del CMC, escriba lo siguiente:

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisServerBasedPowerMgmtMode 0
  ```

Para obtener más información acerca de los comandos de RACADM para la alimentación del chasis, consulte las secciones **config**, **getconfig**, **getpbinfo** y **cfgChassisPower** de *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX).

Ejecución de las operaciones de control de alimentación

Puede ejecutar la siguiente operación de control de alimentación para chasis, servidores y módulos de E/S.

NOTA: Las operaciones de control de alimentación afectan a todo el chasis.

Ejecución de operaciones de control de alimentación en el chasis

El CMC le permite realizar de manera remota varias acciones de administración de la alimentación, por ejemplo, un apagado ordenado, en todo el chasis (el chasis, los servidores, los módulos de E/S y las unidades de suministro de energía).

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de Administrador de control del chasis.

Ejecución de operaciones de control de alimentación en el chasis mediante la interfaz web

Para ejecutar operaciones de control de alimentación en el chasis mediante la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción del chasis** > **Alimentación** > **Control**.
Aparecerá la página **Control de alimentación del chasis**.
2 Seleccione una de las siguientes operaciones de control de alimentación.
Para obtener información sobre cada opción, consulte la *Ayuda en línea*.
- **Encender el sistema**
- **Apagar el sistema**
- **Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)**
- **Restablecer la CMC (reinicio mediante sistema operativo)**
- **Apagado no ordenado**

3 Haga clic en **Aplicar**.
Aparecerá un cuadro de diálogo que solicita confirmación.
4 Haga clic en **Aceptar** para realizar la acción de administración de la alimentación (por ejemplo, hacer que se restablezca el sistema).

Ejecución de operaciones de control de alimentación en el chasis mediante RACADM

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

```
racadm chassisaction -m chassis <action>
```

donde <*action*> es powerup, powerdown, powercycle, nongraceshutdown o reset.

Ejecución de operaciones de control de alimentación en un servidor

Es posible realizar acciones de administración de alimentación de forma remota para varios servidores a la vez o un servidor individual en el chasis.

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de Administrador de configuración del chasis.

Ejecución de operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC

Para ejecutar operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del servidor** > **Alimentación**.

Aparecerá la página **Control de alimentación**.

2 En la columna **Operaciones**, en el menú desplegable, seleccione una de las siguientes operaciones de control de alimentación para los servidores requeridos:

- **Sin operación**
- **Encender el servidor**
- **Apagar el servidor**
- **Apagado ordenado**
- **Restablecer el servidor (reinicio mediante sistema operativo)**
- **Ciclo de encendido del servidor (reinicio mediante suministro de energía)**

Para obtener más información acerca de estas opciones, consulte *Online Help*.

3 Haga clic en **Aplicar**.

Aparecerá un cuadro de diálogo que solicita confirmación.

4 Haga clic en **Aceptar** para ejecutar la acción de administración de alimentación (por ejemplo, restablecer el servidor).

Ejecución de operaciones de control de alimentación en el módulo de E/S

Es posible restablecer o encender de forma remota un módulo de E/S.

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de Administrador de configuración del chasis.

Ejecución de operaciones de control de alimentación en módulos de E/S mediante la interfaz web del CMC

Para ejecutar operaciones de control de alimentación en el módulo de E/S:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del módulo de E/S** > **Alimentación**.

2 Para el módulo de E/S, en la página **Control de alimentación** seleccione desde el menú desplegable la operación que desea ejecutar (ciclo de encendido).

3 Haga clic en **Aplicar**.

Ejecución de operaciones de control de alimentación en el módulo de E/S mediante RACADM

Para ejecutar operaciones de control de alimentación en el módulo de E/S mediante RACADM, abra una consola de texto de serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm chassisaction -m switch <action>
```

en donde *<action>* indica la operación que desea ejecutar: ciclo de encendido.

15

Administración del almacenamiento del chasis

En Dell PowerEdge VRTX, es posible realizar las siguientes operaciones:

- Ver el estado de las unidades de discos físicos y controladoras de almacenamiento.
- Ver las propiedades de las controladoras, las unidades de discos físicos, los discos virtuales y los gabinetes.
- Configurar controladoras, unidades de discos físicos y discos virtuales.
- Asignar adaptadores virtuales.
- Solucionar problemas en controladoras, unidades de discos físicos y discos virtuales.
- Actualizar componentes de almacenamiento.
- Usar las controladoras de almacenamiento compartido en modo con tolerancia a errores
- Activación o desactivación de PERC8 compartido (integrado 2)

NOTA: Inicialización rápida o Inicialización completa no se muestra cuando los discos virtuales se crean inicialmente.

Temas:

- Borrado criptográfico
- Aplicación de la política de acceso para adaptadores virtuales a discos virtuales
- Modificación de las propiedades de disco virtual mediante la interfaz web del CMC
- Módulo de administración de gabinete
- Visualización de las propiedades del gabinete mediante la interfaz web del CMC

Visualización del estado de los componentes de almacenamiento

Para ver el estado de los componentes de almacenamiento:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Propiedades** > **Descripción general del almacenamiento**.

2 En la página **Descripción general del almacenamiento**, es posible:
   - Ver el resumen gráfico de las unidades de discos físicos instaladas en el chasis y su estado.
   - Ver el resumen de todos los componentes de almacenamiento con enlaces a sus respectivas páginas.
   - Ver la capacidad utilizada y la capacidad total del almacenamiento.
   - Ver información de la controladora.

   NOTA: En el caso de una controladora con tolerancia a errores, el formato del nombre es: *<número PERC> (<número> integrado)*. Por ejemplo, la controladora activa es PERC8 compartida (integrada 1) y la controladora homóloga es PERC8 compartida (integrada 2).

   NOTA: Si la controladora PERC está desactivada, el nombre se muestra como PERC desactivada (integrada 2).
   - Ver los sucesos de almacenamiento registrados recientemente.

NOTA: Para obtener más información, consulte la *Ayuda en línea*.

Visualización de la topología de almacenamiento

Para ver la topología de almacenamiento:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Propiedades** > **Topología**.

2 En la página **Topología**, haga clic en el **<nombre de la controladora>** para ver las páginas correspondientes.

   NOTA: Puede ver el nombre de la controladora que está activa al controlar los dispositivos de almacenamiento asociados con este CMC y también la controladora pasiva que actúa como controladora en espera.

3 En cada controladora instalada, haga clic en los vínculos **Ver discos virtuales**, **<nombre del gabinete>** y **Ver discos físicos** para abrir las páginas correspondientes.

Visualización de la información de solución de problemas con tolerancia a errores de SPERC mediante la interfaz web del CMC

Para ver los atributos que indican el correcto funcionamiento de las funciones con tolerancia a errores de una SPERC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Solución de problemas** > **Solución de problemas de configuración**.

   Aparece la página **Solución de problemas de configuración del almacenamiento**.

2 En la página **Solución de problemas de configuración del almacenamiento**, puede:
   - Haga clic en el ⊞ para ver los siguientes atributos cuando la controladora integrada está en modo con tolerancia a errores:

- Dos PERC compartidas detectadas.
- Dos expansores detectados
- PERC compartidas y expansores cableados correctamente
- Firmware correcto en las PERC compartidas
- Firmware correcto en los expansores
- Firmware correcto en la infraestructura del chasis
- Las PERC compartidas tienen la misma configuración: indica si las controladoras SPERC tienen la misma configuración.

- Haga clic en el + para ver los siguientes atributos cuando la controladora integrada no está en el modo con tolerancia a errores:
  - Una PERC compartida detectada.
  - Un expansor detectado
  - PERC compartida y expansores cableados correctamente
- Haga clic en el + para ver los siguientes atributos cuando la controladora externa está en modo con tolerancia a errores:
  - Dos PERC compartidas detectadas
  - Las PERC compartidas están instaladas en diferentes redes fabric
  - Las PERC compartidas y los EMM están conectados correctamente
  - Firmware correcto en las PERC compartidas
  - Las PERC compartidas tienen los mismos valores
- Haga clic en el + para ver los siguientes atributos cuando la controladora externa no está en el modo con tolerancia a errores:
  - Una PERC compartida detectada.
  - Un expansor detectado
  - PERC compartida y expansores cableados correctamente
- Vea el estado de cada atributo que indica si se ha cumplido con los criterios de la tolerancia a errores.

NOTA: Si el atributo del entorno con tolerancia a errores no coincide con el criterio, aparece la opción Actualizar ahora para ese atributo.

NOTA: Aparece la opción Más información para algunos de los atributos. Para obtener más información sobre el atributo, haga clic en Más información.

3 Para cumplir con el criterio de un atributo, haga clic en **Actualizar ahora**.

Aparece la página **Actualización del componente de almacenamiento**, que le permite actualizar el componente de almacenamiento requerido para cumplir con el criterio del atributo.

Asignación de adaptadores virtuales para ranuras mediante la interfaz web del CMC

Si usa la función Adaptador virtual, puede compartir el almacenamiento instalado con los cuatro servidores. Para asignar un disco virtual a una ranura de servidor, primero debe asignar un disco virtual a un adaptador virtual (VA) y, a continuación, un adaptador virtual (VA) a una ranura de servidor.

- Antes de asignar un adaptador virtual a una ranura de servidor, asegúrese de lo siguiente:
  - La ranura del servidor debe estar vacía o el servidor de esa ranura debe estar apagado.
  - Se desasignó el adaptador virtual de un servidor o de una ranura.
  - Todos los servidores afectados están apagados.
- Los discos virtuales se crean y se asignan como **Adaptador virtual 1**, **Adaptador virtual 2**, **Adaptador virtual 3**) o **Adaptador virtual 4**. Para obtener más información, consulte Aplicación de la política de acceso para adaptadores virtuales a discos virtuales.

NOTA:

- Solamente puede asignarle un adaptador virtual a un servidor por vez.
- Sin una licencia adecuada, puede desasignar solo una asignación de adaptador virtual-servidor o asignar el adaptador virtual al servidor predeterminado.
- La asignación predeterminada es adaptador virtual 1-ranura de servidor 1, adaptador virtual 2-ranura de servidor 2, adaptador virtual 3-ranura de servidor 3 y adaptador virtual 4-ranura de servidor 4.
- Si se inserta un servidor de altura completa, la ranura superior tiene el adaptador virtual asignado mientras que la ranura inferior aún está sin asignar. Por ejemplo, un servidor de altura completa en la ranura 1 tiene el adaptador virtual 1 asignado a la ranura 1 y el adaptador virtual 3 sin asignar.
- Si el sistema tiene una licencia Enterprise, puede asignar cualquiera de los cuatro adaptadores virtuales a una ranura de servidor. Sin embargo, aún puede asignar un adaptador virtual a un servidor a la vez.
- Las reglas del adaptador virtual se aplican a los adaptadores de almacenamiento compartido integrados y externos.

Para asignar o desasignar un adaptador virtual de una ranura de servidor:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Configuración** > **Virtualización**.

Aparece la página **Virtualización del almacenamiento**.

2 Para seleccionar el tipo de asignación necesario, desde la tabla **Modo de asignación: discos virtuales a adaptadores virtuales**, seleccione:
   - **Asignación individual**: seleccione esta opción para asignar un disco virtual a un adaptador virtual.
   - **Asignación múltiple**: seleccione esta opción para asignarle un disco virtual a varios adaptadores virtuales. Lea las instrucciones en pantalla antes de seleccionar esta opción.

   NOTA: Seleccione el modo Asignación múltiple solo cuando los servidores tienen los servicios de clúster instalado. El uso de este modo sin los servicios de clúster puede provocar una pérdida de datos o dañarlos.

   NOTA: Puede asignar un disco virtual a varios adaptadores virtuales desde la CLI de la CMC incluso cuando el Modo de asignación está establecido en Asignación individual en la interfaz web de la CMC.

3 En la tabla **Adaptadores virtuales asignados**, en el menú desplegable **Acción**, seleccione una de las siguientes opciones y, a continuación, haga clic en **Aplicar**.
   - **<Nº ranura>**: seleccione la ranura a la que se le debe asignar el adaptador virtual.
   - **Desasignar**: seleccione esta opción para eliminar la asignación del adaptador virtual a una ranura.

   El adaptador virtual se asigna o desasigna de la ranura de servidor seleccionada según la acción seleccionada.

   NOTA: Tenga en cuenta un adaptador virtual asignado al servidor en la ranura inferior (3 o 4). Cuando se reemplaza un servidor de mitad de altura (ranura 3 o 4) por un servidor de altura completa, este último no accede al adaptador virtual asignado a las ranuras inferiores. Si inserta un servidor de mitad de altura de nuevo, se puede acceder al adaptador virtual.

   Asignar o desasignar una controladora PERC virtual al servidor blade:
   - Cada tarjeta PERC 8 compartida externa dispone de cuatro adaptadores virtuales (VA). Si hay una o dos tarjetas PERC 8 compartidas externas presentes en el sistema, en el modo compartido puede asignar o desasignar uno de los cuatro adaptadores virtuales.
   - Si una ranura PCIE externa está ocupada por un adaptador compartido, la asignación del adaptador virtual puede obtener los detalles o la información actuales de la asignación de AV del grupo de AV de almacenamiento compartido.
   - El dispositivo compartido no se admite cuando la ranura del PCIE externo está ocupada por un adaptador compartido. Mediante el adaptador compartido, puede admitir un dispositivo compartido cambiando el conjunto del adaptador virtual del almacenamiento compartido.

Tolerancia a errores en las controladoras de almacenamiento

La Alta disponibilidad (HA) de almacenamiento permite la disponibilidad de varios componentes integrados y varios puntos de acceso a los recursos de almacenamiento. Si un componente de almacenamiento deja de funcionar, el servidor es admitido por un segundo componente

crítico o por la ruta de acceso a los datos disponibles. La alta disponibilidad solamente minimiza el tiempo de inactividad ya que restaura servicios detrás de escena, en la mayoría de los casos antes de que la no funcionalidad sea visible, pero no elimina el tiempo de inactividad. La Tolerancia a errores (FT) utiliza componentes redundantes dentro de un sistema de almacenamiento, que están configurados para actuar como componentes de copia de seguridad y se mantienen en modo de espera. Las controladoras de almacenamiento en modo con tolerancia a errores evitan la disrupción de los servicios de almacenamiento y toman automáticamente los servicios del componente que ha dejado de funcionar. El rendimiento sigue siendo constante a través de este proceso de conmutación por error dado que los componentes redundantes (controladoras) no se usan durante condiciones normales de funcionamiento.

La alta disponibilidad con tolerancia a errores ofrece los siguientes beneficios:

- Proporciona tiempo de actividad para todas las aplicaciones de almacenamiento incluso cuando una controladora deja de funcionar.
- Proporciona acceso a funciones críticas del chasis en todo momento.
- Activa el servidor para manejar situaciones de falla cuando la controladora deja de funcionar.
- Usa la redundancia de los componentes

Si utiliza la función de tolerancia a errores de las controladoras, puede administrar las tareas asociadas con el almacenamiento compartido que se consigue al tener una controladora (homóloga) activa y pasiva. La controladora activa es la controladora que supervisa todos los procesos relacionados con el almacenamiento. El estado de funcionamiento de ambas controladoras se comunica entre las controladoras de modo que, cuando la controladora activa deja de funcionar, la controladora pasiva actúa como repuesto dinámico homólogo, es decir, toma el control sin problemas.

NOTA: La CMC muestra datos de tolerancia a errores de Shared PERC 8 con firmware activado SR-IOV. Si hay una tarjeta no perteneciente a SR-IOV conectada a las ranuras de almacenamiento compartido, la tarjeta no se enciende y se genera una alerta.

NOTA: Operaciones como, por ejemplo, restablecer la CMC, que restablecen la configuración de la CMC, restablecen la configuración externa con tolerancia a errores. Como resultado, el modo PERC cambia a "modo seguro". Desactive la tolerancia a errores en el PERC externo.

Discrepancia de clave de seguridad

Puede crear una clave de seguridad en una controladora mediante una **ID de clave de cifrado** y una **frase de contraseña**. El controlador compara solo la **Frase de contraseña** que se utilizó al crear una clave de seguridad para identificar si las dos controladoras tienen las mismas claves de seguridad. Por lo tanto, dos controladoras que se unen a un clúster cuentan con tolerancia a errores incluso si tuvieran diferentes **ID de clave de cifrado**, siempre y cuando tengan la misma frase de contraseña.

Si se detecta una discrepancia de clave de seguridad entre dos controladoras homólogas, el modo de tolerancia a errores cambia a 'Degradado'. Una alerta crítica se muestra en la página **Condición del chasis** y es posible que la supervisión no muestre una asociación correcta de unidades.

Si se detecta una incompatibilidad de claves de seguridad, resuélvala creando, modificando o eliminando la clave de seguridad en una de las controladoras antes de realizar cualquier otra operación de seguridad de almacenamiento en la controladora. Realice un ciclo de encendido del chasis después de resolver la incompatibilidad. Antes de combinar dos controladoras de disponibilidad no alta, modifique las claves para que coincidan. Esta acción permite importar unidades seguras asociadas con cada controladora que se une al clúster.

Para las controladoras externas, modifique las claves para que coincidan antes de cablearlas para la tolerancia a errores. La modificación de las claves de seguridad permite importar unidades seguras asociadas con cada controladora que se une al clúster.

Resolución de discrepancias en la clave de seguridad mediante la interfaz web de la CMC

Para resolver la incoherencia en la clave de seguridad mediante la interfaz web de la CMC:

1 Apague los módulos de servidor.
2 Haga clic en **Descripción general del servidor** > **Control de** > **alimentación** > **Apagar el servidor**.

3 Modifique la clave de seguridad en una o ambas controladoras sin tolerancia a errores de modo que las claves coincidan.
4 Realice un ciclo de encendido del chasis.
5 Compruebe si las controladoras tienen claves coincidentes.

Visualización de las propiedades de la controladora mediante la interfaz web del CMC

Para ver las propiedades de la controladora:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Controladora**.
2 En la página **Controladoras**, en la sección **Controladoras**, es posible ver las propiedades básicas de la controladora. Sin embargo, para ver las propiedades avanzadas, haga clic en el .

NOTA: Si las controladoras están en modo con tolerancia a errores, también aparece la siguiente información sobre el estado y el modo de la tolerancia a errores:

- Modo con tolerancia a errores: compartido, activo/pasivo
- Estado con tolerancia a errores: satisfactorio/normal o perdido/degradado
- Controladora homóloga: indica el nombre de la controladora que actúa como homóloga (en espera) en el caso de un modo con tolerancia a errores admitido por dos controladoras.

NOTA: Si la controladora homóloga está desactivada, el nombre se muestra como PERC desactivada (integrada 2) o PERC desactivada (SPERC ranura 6) y el estado se muestra como Desconocido, lo que implica que la controladora homóloga está apagada.

Para obtener más información acerca de las controladoras, consulte la *Ayuda en línea*.

Visualización de las propiedades de las controladoras mediante RACADM

Para ver las propiedades de las controladoras mediante RACADM, ejecute el comando `racadm raid get controllers -o`

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Importación o borrado de configuración ajena

Debe insertarse un disco ajeno en el chasis.
Para importar o borrar la configuración ajena:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Controladoras** > **Configuración**.
2 En la página **Configuración de la controladora**, en la sección **Configuración ajena**, para la controladora correspondiente haga clic en:
- **Borrar configuración ajena** para borrar la configuración actual del disco.
- **Importar/Recuperar** para importar el disco con la configuración ajena.

NOTA: Cuando extraiga los discos de un disco virtual específico, restablezca la controladora y vuelva a insertar las unidades en forma individual. Se mostrarán varios ejemplos de discos virtuales de diferentes tamaños y estados en la página Configuración externa. El estado y tamaño correctos del disco virtual se mostrarán después de que la actividad de importación se haya completado.

Configuración de los valores de la controladora de almacenamiento

Puede modificar las propiedades existentes de una controladora de almacenamiento o configurar las propiedades de una controladora de almacenamiento recién instalada.

Configuración de los valores de la controladora de almacenamiento mediante la interfaz web del CMC

Asegúrese de que haya al menos una controladora de almacenamiento instalada en el chasis.
Para configurar los valores de la controladora de almacenamiento:

1 En la interfaz web de la CMC, vaya a **Descripción general del chasis** > **Almacenamiento** > **Controladoras** > **Configurar**.

2 En la página **Configuración de la controladora**, desde el menú desplegable **Controladora**, seleccione la controladora.

NOTA: Tenga en cuenta lo siguiente:

- Si las controladoras de almacenamiento están en modo con tolerancia a errores y si ambas tienen la misma versión de firmware, las dos aparecen como un solo dispositivo en el menú desplegable. Por ejemplo, PERC8 compartida (Integrada 1), PERC8 compartida (Integrada 2), PERC8 compartida (Ranura 5 de SPERC) o PERC8 compartida (Ranura 6 de SPERC). Si la configuración de las dos controladoras es diferente, el mensaje **Configuración incompatible** aparecerá. Puede establecer las propiedades de las controladoras con tolerancia a errores de modo que las propiedades sean iguales en ambas controladoras. Las controladoras en este modo no pueden tener distintas propiedades.
- Si se instala una segunda controladora de almacenamiento con otra versión de firmware, las controladoras aparecen como dos componentes distintos en el menú desplegable. Por ejemplo, PERC8 compartida (Integrada 1), PERC8 compartida (Integrada 2), PERC8 compartida (Ranura 5 de SPERC) y PERC8 compartida (Ranura 6 de SPERC).

Los valores de atributos para la controladora seleccionada se actualizan en la tabla.

3 Escriba o seleccione los datos adecuados y, a continuación, haga clic en **Aplicar**.

NOTA: Para obtener información sobre los atributos y las descripciones de otros campos, consulte la *Ayuda en línea*.

Las propiedades configuradas recientemente se aplican a las controladoras seleccionadas y el campo **Valor actual** muestra los valores actualizados para los atributos.

Configuración de los valores de la controladora de almacenamiento mediante RACADM

Para configurar la controladora de almacenamiento mediante la ejecución de un comando de RACADM, utilice la sintaxis siguiente.

```
racadm raid ctrlprop:RAID.ChassisIntegrated.1-1 [-rebuild <value>] [-bgi <value>] [-reconstruct
<value>] [-checkconsistency <value>] [-ccmode {abortonerror | normal}] [-copybackmode {off | on
| onwithsmart}] [-lb {auto | disabled}] [-prunconfigured {yes | no}]
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Controladoras PERC compartidas

Para los sistemas con dos PERC compartidas integradas instaladas, puede cambiar el modo de funcionamiento de **Con tolerancia a errores** al modo **Sin tolerancia a errores**, o al revés, mediante la interfaz web o la CLI de RACADM. Para ello, active o desactive la segunda controladora PERC 8 compartida interna.

Para la controladora PERC8 compartida interna, puede deshabilitar la segunda controladora integrada. Después de desactivar la segunda controladora integrada, la primera controladora integrada no estará en modo de tolerancia a errores. Cuando la segunda controladora integrada está activada, las controladoras integradas están en modo de tolerancia a errores, de manera predeterminada. La segunda controladora integrada puede desactivarse con el comando. `racadm raid disableperc:RAID.ChassisIntegrated.2-1`

Para los gabinetes externos, ambas tarjetas PERC 8 compartidas externas en las ranuras 5 y 6 se pueden desactivar mediante el comando `racadm raid disableperc: RAID.ChassisSlot.5-1 and racadm raid disableperc: RAID.ChassisSlot.6-1`, respectivamente.

Desde la interfaz de línea de comandos de RACADM, ejecute el comando `racadm raid get controllers` para nombrar la cantidad de controladoras PERC compartidas en el sistema. Si el comando enumera solamente `RAID.ChassisIntegrated.1-1`, significa que el sistema tiene una única controladora PERC compartida. Si el comando enumera `RAID.ChassisIntegrated.1-1`, `RAID.ChassisIntegrated.2-1`, el sistema tiene dos controladoras PERC compartidas.

Se puede activar o desactivar las segunda tarjetas PERC 8 compartida integrada y PERC 8 compartida externa en la ranura 5 y 6.

Para cambiar el modo de funcionamiento mediante la interfaz web de la CMC, vaya a la página **Solución de problemas de controladoras**; para ello, vaya a **Descripción general del chasis** > **Controladoras de almacenamiento** en el panel izquierdo y seleccione la opción **Desactivar controladora RAID** o **Activar controladora RAID**.

Para cambiar el modo de funcionamiento mediante la CLI de RACADM:

- Ejecute el comando `racadm raid enableperc:RAID.ChassisIntegrated.2-1` para activar la **PERC 8 compartida integrada 2** y el modo **Con tolerancia a errores** si la segunda PERC 8 compartida integrada está desactivada.
- Ejecute el comando `racadm raid enableperc:RAID.ChassisSlot.6-1` para activar la **PERC8 compartida externa** en la ranura 6.
- Ejecute el comando `racadm raid disableperc:RAID.ChassisIntegrated.2-1` para desactivar la **Segunda PERC8 compartida integrada** y el modo **Con tolerancia a errores**.

NOTA:

- El chasis debe estar encendido y todos los módulos del servidor deben estar apagados antes de ejecutar los comandos de activar o desactivar. El chasis pasa automáticamente por un ciclo de encendido como parte de esta operación. Después de cambiar el modo de funcionamiento de la PERC compartida, se recomienda restablecer la CMC por medio de la página **Resolución de problemas** o el comando. `racadm racreset`
- De manera predeterminada, si se descubren las segundas tarjetas PERC 8 integradas, el modo muestra el modo de alta disponibilidad.
- La activación de la SPERC en las ranuras externas no activa la tolerancia a errores.
- Para activar el modo con tolerancia a errores para PERC 8 compartida externa, consulte la sección *Activar o desactivar la tolerancia de errores de la controladora RAID externa mediante RACADM* .

Activación o desactivación de alertas mediante la interfaz web del CMC

Para un chasis VRTX con dos controladoras PERC8 compartidas, el adaptador PERC 2 integrado se puede desactivar o activar cuando el adaptador PERC 1 integrado esté activo y todos los módulos de servidor se encuentren apagados. Ambos adaptadores deben estar habilitados para la tolerancia a errores. La página **Solución de problemas de las controladoras** le permite activar o desactivar la controladora homóloga.

NOTA: Para evitar la pérdida de datos, antes de realizar operaciones de activación o desactivación de la controladora:

- Complete todas las operaciones de datos como Reconstrucción o Volver a copiar.
- Asegúrese de que los volúmenes de datos se encuentren en estado óptimo.

NOTA: Al activar el segundo adaptador PERC, aparecerá un mensaje de advertencia y el estado de tolerancia a fallas se degrada si:

- Se cambia cualquiera de los valores del adaptador PERC.
- Se actualiza el firmware.

Asegúrese de que el firmware y la configuración del PERC compartido coincidan a fin de establecer la configuración de tolerancia a fallas en el modo de tolerancia a fallas.

Puede desactivar una controladora homóloga únicamente si:

- Se apagan todos los servidores que están en el chasis.
- La PERC 1 integrada es actualmente la controladora activa.

  NOTA: Si la PERC 1 integrada actualmente no es la controladora activa, realice un ciclo de encendido del chasis para hacer que sea la controladora activa.
- Ambos CMC tienen la misma versión de firmware que admite esta función.

NOTA: Después de desactivar la PERC 2 integrada, en caso de tener que sustituir una tarjeta de la CMC, se recomienda actualizar la tarjeta de la CMC con firmware versión 1.35 o posterior antes de asignar la tarjeta para que sea la controladora CMC activa en el sistema. Aparece un mensaje antes de llevar a cabo esta acción.

Para activar o desactivar una controladora homóloga en modo de tolerancia a fallas mediante la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Controladoras** > **Solución de problemas**.

2 En la página **Solución de problemas de la controladora**, en el menú desplegable **Acciones** para PERC 2 integrado, seleccione una de las siguientes opciones y haga clic en **Aplicar**.

- **Desactivar controladora RAID**: desactiva la controladora homóloga en el modo con tolerancia a errores.
- **Activar controladora RAID**: desactiva la controladora homóloga en modo con tolerancia a errores. Si PERC integrado 2 ya está desactivado, la opción **Activar controladora RAID** está disponible en el menú desplegable.
- Para activar o desactivar las controladoras de tarjeta PERC 8 compartida externa:
  - En la página **Solución de problemas de la controladora**, en el menú desplegable **Acciones** para la tarjeta de PERC 8 compartida externa de la ranura 5 o la ranura 6, seleccione una de las siguientes opciones y, a continuación, haga clic en **Aplicar**.
    - **Desactivar controladora RAID**: desactiva la controladora RAID.
    - **Activar controladora RAID**: activa la controladora homóloga. Si PERC ya está desactivado, la opción **Activar controladora RAID** está disponible en el menú desplegable.
- **Restablecer configuración**: Seleccione esta opción para eliminar la unidad virtual y desasignar todos los repuestos dinámicos conectados a la controladora. Esta operación solamente elimina los discos de la configuración; no borra ningún dato. NOTA: al restablecer la configuración no se eliminan configuraciones ajenas. Use Borrar configuración ajena para restablecer.
- **Exportar registro de TTY**: Seleccione esta opción para exportar el registro de TTY en el sistema local. NOTA: el registro de TTY recopilado de la controladora no contiene datos de las unidades de disco. Sin embargo, puede contener datos tales como direcciones SAS.
- **Activar tolerancia a errores**: seleccione esta opción para activar el modo de tolerancia a errores de la SPERC externa. Esta acción también reinicia la tarjeta PERC 8 compartida externa.
- **Desactivar tolerancia a errores**: seleccione esta opción para desactivar el modo de tolerancia a errores de la SPERC externa. Esta acción también reinicia la tarjeta PERC 8 compartida externa.

NOTA:

- Para una PERC desactivada, ninguna de las demás opciones Restablecer configuración, Exportar registro de TTY, Descartar caché anclada y Desactivar controladora RAID están disponibles en el menú desplegable.
- De manera predeterminada, los dos adaptadores de almacenamiento compartido integrado se detectan con modo de alta disponibilidad.
- Debe activar **Modo de tolerancia a errores** en la controladora compartida externa después de que está conectada.
- **Activar tolerancia a errores** y **Desactivar tolerancia a errores** aparecen solo para las tarjetas PERC 8 compartidas externas. El modo predeterminado de la PERC 8 compartida externa es el modo sin tolerancia a errores.

NOTA: Al activar o desactivar una controladora homóloga, se inicia un ciclo de encendido del chasis. Los cambios se reflejarán solo después de que se complete el ciclo de encendido.

Activación o desactivación de la controladora RAID mediante RACADM

Para activar una controladora homóloga mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm raid enableperc:<AdapterFQDD>
```

Para desactivar una controladora homóloga, introduzca:

```
racadm raid disableperc:<AdapterFQDD>
```

NOTA: Para obtener más información sobre esta función mediante la interfaz de RACADM, consulte *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de línea de comandos de RACADM para iDRAC y CMC).

Activación o desactivación de la tolerancia de errores de controladora RAID externa mediante RACADM

Para activar la tolerancia a errores:

```
racadm raid controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode ha
```

Para desactivar la tolerancia a errores:

```
racadm raid set controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode None
```

Visualización de las propiedades del disco físico mediante la interfaz web del CMC

Asegúrese de que los discos físicos estén instalados en el chasis.
Para ver las propiedades de las unidades de disco físico:

1 En el panel izquierdo, vaya a **Descripción general del chasis** > **Almacenamiento** > **Discos físicos**.
Aparecerá la página **Propiedades**.

2 Para ver las propiedades de todas las unidades de disco físico, en la sección **Disco físico** haga clic en el .

NOTA: Se muestran los siguientes atributos para el modo con tolerancia a errores de los adaptadores compartidos integrados:

- Controladora activa: Shared PERC8 (integrada 1)
- Controladora redundante/contra fallas: Shared PERC8 (integrada 2)

Se muestran los siguientes atributos para el modo con tolerancia a errores de los adaptadores compartidos externos:

- Controladora activa: PERC8 compartida (SPERC ranura 5)
- Controladora redundante o de protección contra fallas: PERC8 compartida (SPERC ranura 6)

También puede utilizar los siguientes filtros para ver las propiedades de unidades de disco físico específicas:

- En la opción **Filtro básico de discos físicos** del menú desplegable **Agrupar por**, seleccione **Disco virtual**, **Controladora** o **Gabinete**, y luego haga clic en **Aplicar**.
- Haga clic en **Filtro avanzado**, seleccione los valores de los diversos atributos y luego haga clic en **Aplicar**.

Visualización de propiedades de unidades de discos físicos mediante RACADM

Para ver las propiedades de las unidades de discos físicos mediante RACADM, ejecute el comando `racadm raid get pdisks —o`

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Identificación de discos físicos y discos virtuales

Para obtener más información acerca de cómo activar o desactivar la función de parpadeo de LED, consulte:

- Configuración del parpadeo de LED mediante la interfaz web del CMC
- Configuración del parpadeo de LED a través de RACADM

Asignación de repuestos dinámicos globales mediante la interfaz web del CMC

Para asignar o desasignar un repuesto dinámico global:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Disco físico** > **Configuración**.
   Se mostrará la página **Configurar discos físicos**.
2. En la sección **Configurar discos físicos**, menú desplegable **Acciones con discos físicos**, seleccione **Sin asignar** o **Repuesto dinámico global** para cada una de las unidades de disco físico y, a continuación, haga clic en **Aplicar**.

NOTA: La asignación del repuesto activo global se permite solo si al menos un disco virtual se encuentra presente en la controladora correspondiente.

Asignación de repuestos dinámicos globales mediante RACADM

Para asignar un repuesto activo global mediante RACADM, ejecute el comando `racadm raid hotspare: -assign yes -type ghs`

Para obtener más información sobre cómo usar comandos RACADM, consulte la *Guía de referencia sobre líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX*.

Recuperación de discos físicos

Para recuperar un disco físico:

1 En la interfaz web del CMC, vaya a **Descripción general del chasis** > **Almacenamiento** > **Discos físicos** > **Configuración**.

2 En la página **Configuración**, bajo la sección **Recuperar discos físicos**, seleccione el disco físico que se debe recuperar y desde el menú desplegable, seleccione **Recrear unidad**, **Cancelar recreación** o **Forzar en línea** según corresponda y, a continuación, haga clic en **Aplicar**.

Visualización de propiedades de discos virtuales mediante la interfaz web del CMC

Asegúrese de que se hayan creado discos virtuales.
Para ver las propiedades de los discos virtuales:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Discos virtuales** > **Propiedades**.

2 En la página **Propiedades**, de la sección **Discos virtuales**, haga clic en el También puede utilizar los siguientes filtros para ver propiedades específicas de los discos virtuales:

- En la sección **Filtro básico de discos virtuales** del menú desplegable **Controladora**, seleccione el nombre de la controladora y luego haga clic en **Aplicar**.
- Haga clic en **Filtro avanzado**, seleccione los valores de los diversos atributos y luego haga clic en **Aplicar**.

Visualización de propiedades de discos virtuales mediante RACADM

Para ver las propiedades de un disco virtual mediante RACADM, ejecute el comando `racadm raid get vdisks -o`

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Creación de un disco virtual mediante la interfaz web del CMC

De manera predeterminada, la CMC crea discos virtuales sin inicializarlos. No obstante, puede elegir la opción de inicialización rápida para los discos virtuales que se crean sin la inicialización. El proceso de inicialización rápida borra los primeros y últimos 8 MB del disco virtual, con lo que se eliminan los registros de inicio o la información sobre particiones. Debe tener el privilegio de **Administrador de configuración del chasis** para realizar la inicialización rápida.
Asegúrese de que el disco físico esté instalado en el chasis.

NOTA: Al eliminar un disco virtual, se quita el disco virtual de la configuración de la controladora.

Para crear un disco virtual:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Discos virtuales** > **Crear**.

2 En la página **Crear un disco virtual**, sección **Nivel de RAID**, seleccione el nivel de RAID.

3 En la sección **Seleccionar discos físicos**, seleccione el número de unidades de disco físico en función del nivel RAID seleccionado.

4 En la sección **Configurar los valores**, escriba los datos adecuados, seleccione las opciones **Inicializar** y **Cifrar disco virtual** y, a continuación, haga clic en **Crear disco virtual**.

La CMC proporciona una nueva opción, la inicialización, al tiempo que crea discos virtuales. Esta opción le permite crear un disco virtual sin inicialización rápida. De manera predeterminada, se crea el disco virtual con inicialización rápida.

La opción **Inicializar** le permite crear discos virtuales sin la inicialización. Esta opción anula el comportamiento predeterminado en el que se lleva a cabo un proceso de inicialización cuando se crea un disco virtual.

La opción **Cifrar disco virtual** le permite crear discos virtuales seguros en unidades cifrado automático (SED).

NOTA: La opción Cifrar disco virtual se activa solo si la clave de cifrado se ha configurado para la controladora específica en la página Configuración de la controladora.

Administración de claves de cifrado

Un cifrado o clave de seguridad, creado en una controladora, se utiliza para bloquear o desbloquear el acceso a discos virtuales seguros creados en SED. Se puede crear una sola clave de cifrado para cada controladora con funciones de cifrado. Puede crear claves de cifrado; para ello, escriba un identificador de la clave de cifrado y una frase de contraseña, en la página **Configuración de la controladora**. La CMC también le permite modificar las frases de contraseña de clave de cifrado y eliminar las claves de cifrado.

Crear clave de cifrado mediante la interfaz web de la CMC

Puede crear claves cifrado o de seguridad para controladoras si la clave de cifrado está **Sin configurar**.
Para crear una clave de cifrado:

1. En el panel izquierdo, vaya a **Configuración** > **de controladoras de** > **almacenamiento**.
2. En el menú desplegable **Clave de seguridad**, seleccione **Crear clave de seguridad**.
   Aparecerá una ventana emergente.
3. Introduzca la clave de seguridad y la contraseña y haga clic en **Aceptar**.
4. En la página **Configuración de la controladora**, haga clic en **Aplicar**.
   Una vez que se crea la clave de cifrado, el estado de la **Clave de seguridad** cambia a **Activado**.

Creación de claves de cifrado mediante RACADM

Para crear una clave de cifrado mediante la ejecución de un comando RACADM, utilice la sintaxis siguiente:

```
racadm raid createsecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -passwd <passphrase>
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Modificación del identificador de clave de cifrado mediante la interfaz web de la CMC

Puede modificar el identificador de clave de cifrado y la frase de contraseña para las controladoras.
Para modificar un identificador de clave de cifrado y la frase de contraseña:

1. En el panel izquierdo, vaya a **Configuración** > **de controladoras de** > **almacenamiento**.
2. En el menú desplegable **Clave de seguridad**, seleccione **Modificar clave de seguridad**.
   Aparecerá una ventana emergente.
3. Introduzca el identificador de la nueva clave de cifrado y las nuevas frases de contraseña y haga clic en **Aceptar**.
4. En la página **Configuración de la controladora**, haga clic en **Aplicar**.

Modificación del identificador de la clave de cifrado mediante RACADM

Para modificar un identificador de clave de cifrado y una contraseña mediante la ejecución de un comando RACADM, utilice la sintaxis siguiente:

```
racadm raid modifysecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -oldpasswd
<oldpassphrase> -newpasswd <newpassphrase>
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Eliminar una clave de cifrado mediante la interfaz web de la CMC

Sólo puede eliminar las claves de cifrado para una controladora cuando los discos virtuales no están asociados a esta.
Para agregar una clave de cifrado:

1 En el panel izquierdo, vaya a **Configuración** > **de controladoras de** > **almacenamiento**.
2 En el menú desplegable, seleccione **Clave de seguridad** y, a continuación, seleccione **Borrar clave de seguridad**.
Aparece un mensaje de confirmación.
3 Haga clic en **OK** (Aceptar) para continuar.
Después de eliminar la clave de cifrado, todos los SED que no forman parte de los discos virtuales se borran de forma segura. Para obtener más información, consulte la *Ayuda en línea*.

Eliminación de la clave de cifrado mediante RACADM

Para eliminar una clave de cifrado mediante la ejecución de un comando RACADM, utilice la sintaxis siguiente:

```
racadm raid deletesecuritykey:RAID.ChassisIntegrated.1-1
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Cifrado de discos virtuales

Puede cifrar los discos virtuales creados en los SED después de configurar una clave de cifrado en la controladora. Siempre que se realiza un cifrado, se registra un mensaje en el `CMC Log`. Puede cifrar discos virtuales:

- La clave de seguridad se configura en la controladora.
- Todas las unidades en el disco virtual son discos SED.

Cifrar un disco virtual activa el cifrado en todos los discos virtuales en el mismo grupo de discos.

Debe tener privilegios de **Administrador de configuración del chasis** para cifrar discos virtuales.

Cifrado de discos virtuales mediante la interfaz web de la CMC

Para cifrar un disco virtual existente:

1 En el panel izquierdo, haga clic en **Almacenamiento** > **Discos virtuales** > **Administrar**.
2 En el menú desplegable **Acciones virtuales**, seleccione **Cifrar disco virtual** y haga clic en **Aplicar**.

NOTA: La opción Cifrar disco virtual sólo está disponible si los discos virtuales no seguros están configurados en el SED.

Cifrado de discos virtuales con RACADM

Para cifrar discos virtuales mediante la ejecución de un comando de RACADM, utilice la sintaxis siguiente:

```
racadm raid encryptvd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Desbloquear la configuración ajena

Las unidades que forman parte de los discos virtuales seguros se denominan unidades seguras. Las unidades seguras se pueden migrar de una controladora a otra. Si un cifrado o clave de seguridad diferente está configurado para la controladora de destino, el estado de seguridad de estas unidades se muestra como 'bloqueado' y no podrán verse como parte de la 'configuración ajena de vista previa'. La opción 'configuración ajena de importación" no detecta estas unidades ajenas.

Mientras se ejecuta el comando de desbloqueo, debe proporcionar la contraseña de la controladora de origen y la ID de la clave para estas unidades. Incluso después de desbloquear, la "clave de la controladora ajena" continúa asegurando estas unidades. Sin embargo, se pueden ver estas unidades mientras se buscan unidades ajenas en la "configuración ajena de vista previa" existente. Puede importar o borrar la configuración ajena en estas unidades seguras.

Si las unidades ajenas con diferentes claves de seguridad se migran de más de una controladora, se debe desbloquear e importar o borrar el conjunto de unidades de una controladora ajena antes de desbloquear las unidades migradas de otro controlador. Esta acción garantiza que no se permita desbloquear en una controladora si la controladora tiene unidades desbloqueadas pero no importadas o borradas.

Una vez que las unidades se desbloquean, puede importar la configuración ajena mediante la interfaz web de la CMC o RACADM.

Si la controladora está apagada y se ha vuelto a encender después de la fase de desbloqueo y antes de la importación, las unidades se vuelven a bloquear.

Si el sistema tiene varias configuraciones ajenas, desbloquee e importe cada configuración ajena antes de desbloquear la configuración ajena.

La ID de la clave que se utiliza en el desbloqueo se utiliza solamente para identificar las unidades que coinciden con la ID de clave. Después de encontrar las unidades que coinciden, la frase de contraseña se utiliza para desbloquear las unidades.

Desbloqueo de la configuración ajena mediante la interfaz web de la CMC

Para desbloquear la configuración ajena:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Controladoras** > **Configuración**.
2 Visite la página **Configuración**.
3 Haga clic en **Hacer clic aquí para desbloquear**.
Se mostrará la página **Discos físicos**.
4 Seleccione los discos físicos que desee desbloquar.
5 Compruebe si el disco físico está asociado con el identificador de claves.
6 Desde el menú desplegable **Acciones**, seleccione **Desbloquear unidad.**
Aparece un cuadro de diálogo que le pide que introduzca la frase de la clave de seguridad.
7 Introduzca una frase de contraseña en el cuadro de texto **Frase de contraseña de la clave de seguridad**.
8 Vuelva a introducir la frase de contraseña y haga clic en **Desbloquear**.
La unidad física está desbloqueada y la unidad no aparece en la lista **Recuperar discos físicos**.

Desbloquear la configuración externa mediante RACADM

Para desbloquear la configuración externa mediante la ejecución de un comando de RACADM, utilice la sintaxis siguiente:

```
racadm raid unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Borrado criptográfico

Puede utilizar la opción de borrado criptográfico para borrar con seguridad datos que se encuentren en SED seguras. Los datos seguros existen en unidades incluso después de que el disco virtual se elimina y, por lo tanto, quedan expuestos a amenazas. El borrado criptográfico se puede utilizar en las siguientes condiciones:

- Para borrar los datos para retirar/volver a utilizar las unidades seguras.
- Para borrar los datos de forma segura si la configuración externa bloqueada no necesita importarse.
- Para recuperar las unidades bloqueada si se pierde la frase de contraseña.

Puede realizar el borrado criptográfico en uno o más discos físicos SED.

PRECAUCIÓN: Si se realiza la tarea de borrado criptográfico, se borran todos los datos del disco físico.

Realización de borrado criptográfico

Si el disco físico es parte de un disco virtual, extráigalo del disco virtual antes de realizar el borrado criptográfico.
Para realizar un borrado criptográfico:

1 En el panel izquierdo, vaya a **Descripción general del chasis** > **Almacenamiento** > **Discos físicos**.
Se mostrará la página **Configurar discos físicos**.
2 Seleccione el disco físico desde el que desea borrar los datos.
3 En el menú desplegable **Acciones de discos físicos**, seleccione **Borrado criptográfico** y haga clic en **Aplicar**.

Aparece un mensaje que le solicita que confirme la acción.

4 Haga clic en **Sí** para continuar.

Todos los datos de los discos físicos seleccionados se eliminan.

Aplicación de la política de acceso para adaptadores virtuales a discos virtuales

Asegúrese de que las unidades de discos físicos estén instaladas y que se hayan creado discos virtuales.
Para aplicar la política de acceso para adaptadores virtuales:

1 En el panel izquierdo, haga clic en **Descripción del chasis** > **Almacenamiento** > **Discos virtuales** > **Asignar**.

2 En la página **Asignar discos virtuales**, en la sección **Política de acceso para adaptadores virtuales** del menú desplegable **Adaptador virtual <número>**, seleccione **Acceso total** para cada unidad de disco físico.

3 Haga clic en **Aplicar**.

Ahora podrá asignar adaptadores virtuales a ranuras del servidor. Para obtener más información, consulte la sección Asignación de adaptadores virtuales a ranuras de esta Guía del usuario.

Modificación de las propiedades de disco virtual mediante la interfaz web del CMC

Para modificar las propiedades del disco virtual:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Discos virtuales** > **Administrar**.

2 En la página **Administrar discos virtuales**, en el menú desplegable **Acciones del disco virtual**, seleccione una de las siguientes acciones y, a continuación, haga clic en **Aplicar**.

- **Cambiar nombre**
- **Eliminar**

NOTA: Si selecciona Eliminar, se muestra el siguiente mensaje que indica que la eliminación de un disco virtual eliminará de forma permanente los datos disponibles en dicho disco virtual.

```
Deleting the virtual disk removes the virtual disk from the controller's configuration.
Initializing the virtual disk permanently erases data from the virtual disk.
```

- **Política de edición: Caché de lectura**
- **Política de edición: Caché de escritura**
- **Política de edición: Caché del disco**
- **Inicialización: rápida**
- **Inicialización: completa**
- **Cifrar disco virtual**

Módulo de administración de gabinete

El Módulo de administración del gabinete (EMM) proporciona tareas de administración de gabinete y de ruta de datos para el gabinete. EMM supervisa y controla los componentes del gabinete y el acceso a las unidades.

EMM comunica los atributos y estados del gabinete al servidor host Los módulos EMM controlan los siguientes componentes del gabinete:

- Ventiladores
- Fuentes de alimentación
- Sondas de temperatura
- Instalación o extracción de un disco físico

- Indicadores LED en el gabinete

Visualización del estado y los atributos del EMM

El estado del módulo EMM muestra la condición del EMM. Los EMM contienen un valor de estado que es exclusivo del gabinete. Puede tener hasta dos módulos EMM. El firmware del gabinete crea un estado para cada EMM.

Visualización del estado y los atributos de EMM mediante la interfaz web

Para ver el estado y atributos del EMM.

Haga clic en **Descripción general del chasis** → **Almacenamiento** → **Gabinetes** → **Propiedades**. La **página Gabinetes** proporciona el estado del EMM y atributos de los gabinetes en el chasis. Expanda el gabinete integrado o los gabinetes externos para ver el estado y los atributos del EMM. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización del estado y los atributos de EMM mediante RACADM

Para ver el estado de EMM, utilice el comando `racadm raid get emms -o -p Status`.

Para ver los atributos de EMM, utilice el comando `racadm raid get emms -o`.

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en **dell.com/support/manuals**.

Visualización del estado y de los atributos del gabinete

La CMC muestra la condición del gabinete en función de los componentes físicos. Los datos de los gabinetes conectados a un almacenamiento compartido se mostrarán en la CMC, pero los gabinetes externos conectados a algunas tarjetas PCIe no se muestran. Debe tener privilegios de inicio de sesión de la CMC para ver el estado y los atributos de los gabinetes.

Visualización del estado y los atributos del gabinete mediante la interfaz web

Para ver el estado y los atributos del gabinete:

Haga clic en **Descripción general del chasis** → **Almacenamiento** → **Gabinetes** → **Propiedades**. La **página Gabinetes** proporciona el estado de los gabinetes en el chasis. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

NOTA: El estado consolidado del gabinete se vuelve crítico cuando el EMM, la PSU o el ventilador se extraen, pero el estado principal se mantiene de la misma manera. Después de que el CMC o el chasis completan el ciclo de apagado y encendido, el estado principal también se vuelve crítico.

Visualización del estado y los atributos del gabinete mediante RACADM

Para ver el estado del gabinete, utilice el comando `racadm raid get enclosures –o –p Status`.

Para ver los atributos del gabinete, utilice el comando `racadm raid get enclosures –o`.

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en **dell.com/support/manuals**.

Informar un máximo de dos gabinetes por cada conector

Cada tarjeta PERC 8 compartida externa admite hasta dos gabinetes por conector. Sin embargo, existen dos configuraciones diferentes con diferentes restricciones. En una configuración de PERC única (sin tolerancia a errores) se puede conectar hasta dos gabinetes por tarjeta. Debido al cableado redundante, una solución de tarjeta PERC 8 compartida externa con tolerancia a errores admite hasta dos gabinetes por par con tolerancia a errores.

Si se detectan más de dos gabinetes en cualquier conector, se registra un mensaje de advertencia en el registro del chasis. Esto afecta la condición del chasis y proporciona una alerta activa o entrada de registro del chasis.

Configuración de etiqueta de propiedad y nombre de propiedad del gabinete

Para identificar los gabinetes, establezca el nombre de propiedad y la etiqueta de propiedad de los gabinetes.

NOTA:

- Se muestra un error si introduce un valor no válido.
- Inicialmente, se muestra el valor que se guarda en el firmware.
- Debe tener privilegios de configuración del chasis para establecer la etiqueta de propiedad y el nombre de propiedad del gabinete.
- Puede establecer la etiqueta de propiedad y el nombre de propiedad solo para los gabinetes externos.

Configuración de Etiqueta de propiedad y Nombre de propiedad del gabinete mediante la interfaz web

Para establecer la etiqueta de propiedad y el nombre de la propiedad del gabinete, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Gabinetes** → **Configuración**. Escriba la **Etiqueta de propiedad** y el **Nombre de la propiedad** en los campos correspondientes y, a continuación, haga clic en **Aplicar**. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Configuración de la etiqueta de propiedad y el nombre de propiedad del gabinete mediante RACADM

Para establecer etiqueta de propiedad del gabinete, utilice el comando `racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 -p AssetTag <value>`.

Para establecer nombre de la propiedad del gabinete, utilice el comando `racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 -p AssetName <value>`.

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en **dell.com/support/manuals**.

Visualización del estado y los atributos de la sonda de temperatura del gabinete

El estado de la sonda de temperatura muestra el estado de los sensores de temperatura del gabinete. Los sensores contienen un valor de estado que es exclusivo del gabinete. Puede tener hasta cuatro sensores de temperatura o sondas y el firmware del gabinete crea un estado de cada sensor. Debe tener privilegios de inicio de sesión en la CMC para ver el estado de la sonda.

Visualización del estado y los atributos de la sonda de temperatura del gabinete mediante la interfaz web

Para ver el estado y los atributos de la sonda de temperatura del gabinete:

Haga clic en **Descripción general del chasis** → **Almacenamiento** → **Gabinetes** → **Propiedades**. La **página Gabinetes** proporciona el estado y los atributos de la sonda de temperatura del gabinete en el chasis. Expanda el gabinete externo para ver el estado de la unidad de suministro de energía de los gabinetes. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización de los atributos de la sonda de temperatura del gabinete mediante RACADM

Para ver los atributos de la sonda de temperatura del gabinete, utilice el comando `racadm raid get tempprobes -o`. Para obtener más información, consulte la *Guía de referencia de la línea de comando RACADM de Chassis Management Controller para PowerEdge VRTX* que está disponible en **dell.com/support/manuals**.

Configuración del umbral de advertencia de temperatura del gabinete

El umbral de advertencia de temperatura le permite cambiar el umbral en el que la temperatura de un gabinete se informa como de advertencia.

NOTA:

- Se muestra un error si introduce un valor no válido.
- Inicialmente, se muestra el valor que se guarda en el firmware.
- Debe tener privilegios de configuración del chasis para establecer la etiqueta de propiedad y el nombre de propiedad del gabinete.

Configuración del umbral de advertencia de temperatura del gabinete mediante la interfaz web

Para establecer el umbral de advertencia de temperatura del gabinete:

Haga clic en **Descripción general del chasis** → **Almacenamiento** → **Gabinetes** → **Configuración**. Seleccione el gabinete del menú desplegable **Gabinete** y, a continuación, introduzca los valores mínimo y máximo correspondientes para las temperaturas del umbral de advertencia del sensor de temperaturas 2 y 3. Escriba la **etiqueta de propiedad** y el **nombre de la propiedad** en los campos correspondientes y, a continuación, haga clic en **Aplicar**. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para la CMC)*.

Configuración del umbral de advertencia de temperatura del gabinete mediante RACADM

Para establecer el umbral de advertencia mínimo de sonda de temperatura en el gabinete, utilice el comando `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MinimumWarningThreshold <value>`.

Para establecer el umbral de advertencia máximo de sonda de temperatura en el gabinete, utilice el comando `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MaximumWarningThreshold <value>`.

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en **dell.com/support/manuals**.

Visualización del estado y los atributos del ventilador del gabinete

El estado y los atributos del ventilador muestra el estado del ventilador del gabinete y contiene un valor de estado que es exclusivo del gabinete. Puede tener hasta dos ventiladores y el firmware del gabinete crea un estado de cada ventilador. Debe tener privilegios de inicio de sesión en la CMC para ver el estado del ventilador.

NOTA: Si una unidad de suministro de energía no está presente, el ventilador correspondiente de la unidad de suministro de energía muestra un estado crítico.

Visualización del estado y los atributos del ventilador del gabinete mediante la interfaz web

Para ver el estado y los atributos de una unidad de suministro de energía:

Haga clic en **Descripción general del chasis** → **Almacenamiento** → **Gabinetes** → **Propiedades**. La **página del gabinete** proporciona el estado y los atributos para el ventilador del gabinete. Expanda el gabinete externo para ver el estado del ventilador del gabinete. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización del y los atributos del ventilador del gabinete mediante RACADM

Para ver el estado del ventilador, utilice el comando `racadm raid get fans -o -p Status`.

Para ver los atributos del ventilador, utilice el comando `racadm raid get fans -o`.

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) que está disponible en **dell.com/support/manuals**.

Visualización de las propiedades del gabinete mediante la interfaz web del CMC

Para ver las propiedades del gabinete:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Gabinetes** > **Propiedades**.

2 En la página **Propiedades**, en la sección **Gabinete**, haga clic en el  para obtener una visualización gráfica de las unidades de discos físicos y sus estados, un resumen de ranuras de unidades de discos físicos y propiedades avanzadas.

16

Administración de ranuras PCIe

Todas las ranuras están desasignadas de manera predeterminada. Puede hacer lo siguiente:

- Ver el estado de todas las ranuras PCIe del chasis.
- Asignar o quitar una ranura PCIe asignada de los servidores.

Tenga en cuenta lo siguiente antes de asignar una ranura PCIe a un servidor:

- Si una ranura PCIe está vacía, no se la puede asignar a un servidor encendido.
- Una ranura PCIe que tiene un adaptador asignado a un servidor no puede ser asignada a otro servidor si el que está actualmente asignado (servidor fuente) está encendido.
- Una ranura PCIe que tiene un adaptador asignado a un servidor no puede ser asignada a otro servidor (de destino) que está encendido.

Considere lo siguiente antes de extraer una ranura PCIe asignada de un servidor:

- Si una ranura PCIe está vacía, se la puede desasignar de un servidor, incluso si está encendido.
- Si una ranura PCIe tiene un adaptador y este no está encendido, se la puede desasignar del servidor aunque esté encendido. Esto puede ocurrir cuando la ranura está vacía y el servidor asignado está encendido, y un usuario introduce un adaptador en la ranura vacía.

Asignar o desasignar el adaptador PCIe externo al servidor blade:

- El adaptador siempre se enciende como dispositivo no compartido. En lo sucesivo, el adaptador está asignado a un servidor.
- Si una ranura PCIE externa está ocupada por un adaptador compartido, la asignación antes del adaptador que se inserta se mantiene sin cambios.
- Si una ranura PCIE externa está ocupada por un adaptador compartido, la ranura de PCLE puede no asignar o desasignar, en o desde un servidor blade. Si un usuario intenta asignar o desasignar un adaptador compartido, se registra un mensaje EEMI.

Para obtener más información sobre la asignación y eliminación de una ranura PCIe asignada de los servidores, consulte la *Ayuda en línea*.

NOTA:

- Sin una licencia, puede asignar un máximo de cuatro ranuras PCIe a un servidor de altura completa, dos en la ranura superior y dos en la ranura de extensión, o dos dispositivos PCIe a un servidor de mitad de altura.
- Puede distinguir las propiedades de las ranuras PCIE externas con dispositivos de tarjeta PERC 8 compartida externa de los dispositivos dedicados ya que las propiedades de estos dispositivos compartidos son diferentes a las de los dispositivos dedicados.
- En el caso de la SPERC externa, el estado se mostrará como Compartido. Las opciones para asignar o desasignar la tarjeta PERC 8 compartida externa no están disponibles.

Temas:

Visualización de propiedades de ranuras PCIe mediante la interfaz web del CMC

- Para ver la información acerca de las ocho ranuras PCIe, vaya al panel izquierdo y haga clic en **Descripción general del chasis** > **Descripción general de PCIe**. Haga clic en el ⊞ para ver todas las propiedades para la ranura requerida.
- Para ver la información acerca de una ranura PCIe, haga clic en **Descripción general del chasis** > **Ranura de PCIe <número>** > **Propiedades** > **Estado**.

NOTA: La interfaz de usuario diferencia las ranuras PCIe externas que contienen dispositivos SPERC (u otros dispositivos compartidos) instalados desde ranuras PCIe externas con adaptadores dedicados ya que estos dispositivos compartidos poseen propiedades distintas.

Asignación de ranuras PCIe a los servidores mediante la interfaz web del CMC

Para asignar ranuras PCIe a los servidores:

- En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general de PCIe** > **Configuración** > **Asignación: ranuras de PCIe a ranuras de servidor**. En la página **Asignación: ranuras de PCIe a ranuras de servidor**, en la columna **Acción** del menú desplegable **Acción**, seleccione el nombre de servidor adecuado y, a continuación, haga clic en **Aplicar**.

Tenga en cuenta lo siguiente:

- Sin una licencia, se puede asignar como máximo dos ranuras PCIe a un servidor de mitad altura. Si se instala un servidor de altura completa, puede asignar dos ranuras PCIe a la ranura del servidor superior y dos a la ranura del servidor inferior (extendido), para un total de cuatro ranuras PCIe por servidor de altura completa**.**
- Puede asignar las ranuras de servidor a cualquiera de las 8 ranuras PCIe.
- Un servidor de altura completa tiene las tarjetas intermedias superior e inferior ocupadas. De lo contrario, se detendrá durante la POST cuando la <F1> o <F2> aparezca en la página para que pulse cualquier una de las teclas.
- En el caso de los servidores de altura completa, puede asignar un máximo de dos ranuras PCIe a las tarjetas intermedias superiores y dos a las inferiores. De manera predeterminada, todas las asignaciones de PCIe a la ranura 3 del servidor se dirigirán a las tarjetas intermedias inferiores.
- El número de ranura del servidor se muestra como Slot-01, Slot-02, etc. Para un servidor de altura completa, el nombre de ranura aparecerá como Ext. de Slot-01, Ext. de Slot-02, y así sucesivamente.
- Si selecciona el nombre de host, este aparecerá en lugar del nombre de la ranura.
- La CMC proporciona capacidades de alerta a través del Registro de sucesos del sistema (SEL), SNMP y las interfaces de correo electrónico.

Para obtener más información acerca de cómo asignar dispositivos PCIe a un servidor, consulte la *ayuda en línea*.

Administración de ranuras PCIe mediante RACADM

Es posible asignar o desasignar una ranura PCIe a un servidor mediante los comandos RACADM. Algunos de estos comandos se presentan aquí. Para obtener más información acerca de los comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en dell.com/support/manuals.

- Para ver la asignación actual de dispositivos PCIe a servidores, ejecute el siguiente comando:

```
racadm getpiecfg -a
```

- Para ver las propiedades de los dispositivos PCIe mediante FQDD, ejecute el siguiente comando:

  ```
  racadm getpciecfg [-c <FQDD>]
  ```

  Por ejemplo, para ver las propiedades del dispositivo PCIe 1, ejecute el siguiente comando:

  ```
  racadm getpciecfg -c PCIE.ChassisSlot.1
  ```
- Para asignar una ranura de adaptador PCIe a una ranura de servidor, ejecute el siguiente comando:

  ```
  racadm setpciecfg assign [-c <FQDD>] [i <server slot>]
  ```
- Por ejemplo, para asignar la ranura PCIe 5 a la ranura de servidor 2, ejecute el siguiente comando:

  ```
  racadm setpciecfg assign -c PCIE.ChassisSlot.5 -i 2
  ```
- Para desasignar una ranura PCIe 3 de un servidor, ejecute el siguiente comando:

  ```
  racadm setpciecfg unassign -c pcie.chassisslot.3
  ```

Protección de la alimentación de PCIe

Las tarjetas PCIe recién asignadas al CMC VRTX deben descubrirse e inicializarse antes de que se encienda el nodo de un servidor. El proceso de descubrimiento e inicialización incluye lo siguiente:

- Realizar inventario y descubrimiento de las tarjetas instaladas
- Preparar una tarjeta PCIe para la exposición a un módulo de servidor
- Preparar varias tarjetas para la configuración por parte del BIOS del servidor
- Inicialización de todas las tarjetas antes de que se encienda el nodo de un servidor blade

Todos estos procesos tardan algunos segundos en completarse, lo que ocasiona un retraso en la inicialización de las tarjetas PCIe. La función de protección de PCIe en CMC VRTX reduce el tiempo del ciclo de este proceso. La función de protección de PCIe permite lo siguiente:

- Los nodos del servidor se encienden rápidamente y, en consecuencia, también lo hacen las tarjetas PCIe.
- El estado encendido de las tarjetas PCIe se extiende durante un período de tiempo predefinido en los siguientes escenarios:
  - Una vez apagado el servidor asociado.
  - Después de que se complete el proceso de detección del adaptador.
- El estado de encendido de las tarjetas se extiende durante un tiempo predefinido después del proceso de descubrimiento. Esta extensión elimina las demoras para tipos comunes de ciclos de encendido. Las tarjetas siguen estado listas y en espera de la asignación de nodo y del encendido. Las tarjetas se apagan una vez finalizado el período de tiempo.

.

NOTA: Al finalizar el período de tiempo, las tarjetas PCIe se apagan. Todos los adaptadores en el modo de protección también se apagan cuando se abre la puerta del chasis.

NOTA:

- Si el CMC no tiene suficiente alimentación, el CMC apaga todos los adaptadores en el modo de protección, con lo cual se libera toda la alimentación asignada a esos adaptadores. Si la fuente de alimentación se restablece, el consumo de energía se reasigna a las ranuras PCIe. Este tipo de restauración de la alimentación restauración permite que las tarjetas estén listas para la asignación de servidores sin demora.
- Todos los adaptadores PCIE externos encendidos en modo compartido se excluyen de los procesos en modo de protección. Después de que un adaptador compartido se enciende como dispositivo compartido, este permanece encendido hasta que se apague el chasis.

Visualización de propiedades de protección de PCIe mediante la interfaz web del CMC

Para ver las propiedades de protección de PCIe, en el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general de PCIe**. Aparecerá la página **Estado de PCIe**. La sección **Configuración general** muestra los siguientes estados de propiedades de protección de PCIe:

- **Estado de la protección**: activado o desactivado.
- **Tiempo de espera de la protección**: indica el tiempo durante el cual se activa la función de protección

Visualización del estado de las propiedades de protección de PCIe mediante RACADM

Para ver la información acerca de las propiedades de protección de la alimentación de PCIe, introduzca el siguiente comando:

```
racadm getpciecfg –r
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Configuración de las propiedades de protección de PCIe mediante la interfaz web del CMC

Para configurar las propiedades de protección de PCIe para CMC VRTX:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Configuración** > **Protección**.
Aparece la página **Configuración de la protección de PCIe**.

2 Para activar o desactivar la función de protección de PCIe, seleccione o borre la opción **Activar protección de PCIe** .

NOTA: De manera predeterminada, la función de protección está activada y el período de tiempo se establece en 300 segundos.

3 En el campo **Tiempo de espera**, escriba el tiempo durante el cual la función de protección estará activada.
Escriba cero (0) o un valor de 60-1800 segundos. Cero indica un tiempo de espera infinito.

4 Haga clic en **Aplicar**.

Configuración del estado de las propiedades de protección de PCIe mediante RACADM

Puede configurar las propiedades de protección de la alimentación de PCIe mediante la ejecución de los siguientes comandos:

- Para desactivar la función de protección, ejecute el comando `racadm setpciecfg ridethru –d`
- Para activar la función de protección, ejecute el comando `racadm setpciecfg ridethru –e`
- Para restablecer la propiedad de tiempo de espera de protección, ejecute el comando `racadm setpciecfg ridethru –t <timeout>`
- Para establecer el rango de tiempo de espera aceptable, ejecute el comando `racadm setpciecfg help ridethru`

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

17

Solución de problemas y recuperación

En esta sección se explica cómo realizar tareas relacionadas con la recuperación y la solución de problemas en el sistema remoto a través de la interfaz web del CMC.

- Visualización de la información del chasis.
- Visualización de los registros de sucesos.
- Recopilación de información de configuración, estados de errores y registros de errores.
- Uso de la consola de diagnósticos.
- Administración de la alimentación en un sistema remoto.
- Administración de trabajos de Lifecycle Controller en un sistema remoto.
- Restablecimiento de componentes.
- Solución de problemas de protocolo de hora de red (NTP).
- Solución de problemas de red.
- Solución de problemas de alertas.
- Restablecimiento de la contraseña olvidada del administrador.
- Forma de guardar y restablecer los valores de configuración y certificados del chasis.
- Visualización de códigos y registros de errores.

NOTA: La compatibilidad con WinRM para Microsoft no se encuentra disponible para Windows 10 cliente; utilice Power Shell en lugar de WinRM.

Temas:

Restablecimiento de la contraseña administrativa olvidada

El siguiente procedimiento explica cómo restablecer la contraseña administrativa olvidada:

- Quite el módulo de la CMC del chasis.
- Acorte las clavijas de encabezado de **Recuperación de contraseña** mediante el puente.
- Vuelva a insertar el módulo de la CMC en el chasis. Cuando la CMC esté en línea, se activará la credencial predeterminada (nombre de usuario: root/Contraseña: calvin)
- Iniciar sesión en la CMC con la credencial predeterminada y cambiar la contraseña
- Una vez cambiada la contraseña, extraiga módulo de la CMC y el puente del encabezado **Recuperación de contraseña**
- Vuelva a insertar el módulo de la CMC en el chasis. Cuando la CMC esté en línea, se activará la credencial nueva

Recopilación de información de configuración, registros y estado del chasis mediante RACDUMP

El subcomando `racdump` permite utilizar un solo comando para obtener información completa sobre el estado del chasis, datos de estado de configuración y registros históricos de sucesos.

El subcomando `racdump` muestra la siguiente información:

- Información general del sistema/RAC
- Información de la CMC
- Información del chasis
- Información de la sesión
- Información del sensor
- Información de la compilación de firmware

Interfaces admitidas

- RACADM mediante CLI
- RACADM remoto
- RACADM mediante Telnet

`racdump` incluye los siguientes subsistemas e incorpora los siguientes comandos de RACADM. Para obtener más información sobre `racdump`, consulte la *RACADM Command Line Reference Guide for CMC in PowerEdge VRTX* (Guía de referencia de línea de comandos de RACADM para la CMC en PowerEdge VRTX).

Tabla 42. Comandos de racadm para subsistemas

Subsistema	Comando de RACADM
Información general del sistema/RAC	`getsysinfo`
Información de la sesión	`getssninfo`
Información del sensor	`getsensorinfo`
Información de los conmutadores (módulo de E/S)	`getioinfo`
Información de la tarjeta mezzanine (tarjeta subordinada)	`getdcinfo`
Información de todos los módulos	`getmodinfo`
Información del presupuesto de alimentación	`getpbinfo`
Información de KVM	`getkvminfo`
Información del NIC (módulo CMC)	`getniccfg`
Información de redundancia	`getredundancymode`

Subsistema	Comando de RACADM
Información del registro de rastreo	`gettracelog`
Registro de sucesos de RAC	`getraclog`
Registro de sucesos del sistema	`getsel`

Descarga del archivo de Base de información de administración de SNMP

El archivo Base de información de administración de SNMP (MIB) de la CMC define los indicadores, sucesos y tipos de chasis. La CMC permite descargar el archivo MIB a través de la interfaz web.

Para descargar el archivo MIB de SNMP de la CMC a través de la interfaz web de la CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Red** > **Servicios** > **SNMP**.

2 En la sección **Configuración de SNMP**, haga clic en **Guardar** para descargar el archivo MIB de la CMC en el sistema local.

Para obtener más información sobre el archivo MIB SNMP, consulte la *Guía de referencia de SNMP de Dell OpenManage Server Administrator* disponible en **dell.com/support/manuals**.

Primeros pasos para solucionar problemas de un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas de alto nivel en el sistema administrado:

- ¿El sistema se enciende o se apaga?
- Si está encendido, ¿el sistema funciona, no responde o dejó de funcionar?
- Si está apagado, ¿se ha apagado de forma imprevista?

Solución de problemas de alimentación

La información siguiente le ayudará a solucionar problemas de suministro de energía y problemas relacionados con la alimentación:

- **Problema**: se ha configurado **Política de redundancia de alimentación** en la opción **Redundancia de la red eléctrica** y se ha producido un suceso de Redundancia de suministro de energía perdida.
  - **Solución A:** esta configuración requiere que al menos un suministro de energía en el lado 1 (las dos ranuras de la izquierda) y un suministro de energía en el lado 2 (las dos ranuras de la derecha) estén presentes y en estado funcional en el gabinete modular. Asimismo, la capacidad de cada lado debe ser suficiente para soportar el total de asignaciones de energía necesarias para que el chasis mantenga la **Redundancia de cuadrícula**. (Para una plena operación de redundancia de cuadrícula, asegúrese de disponer de una configuración completa de unidades de suministro de energía de cuatro suministros de energía).
  - **Solución B:** revise si todos los suministros de energía están correctamente conectados a las dos redes de CA. Los suministros del lado 1 deben estar conectados a una red de CA y los del lado 2 deben estar conectados a la otra red, y ambas redes de CA deben estar en funcionamiento. La **Redundancia de cuadrícula** se pierde cuando una de las redes de CA no funciona.
- **Problema:** el estado de la unidad de suministro de energía se muestra como **Error (Sin CA),** aun cuando hay conectado un cable de CA y la unidad de distribución de alimentación produce buena salida de CA.
  - **Solución A:** Compruebe y reemplace el cable de CA. Compruebe y confirme que la unidad de distribución de energía que proporciona la alimentación al suministro de energía funcione como se espera. Si no se soluciona el error, comuníquese con la atención al cliente de Dell para reemplazar el suministro de energía.
  - **Solución B:** revise que la unidad de suministro de energía esté conectada al mismo voltaje que las otras unidades. Si el CMC detecta que una unidad de suministro de energía está funcionando con un voltaje distinto, la unidad se apaga y se marca como fallida.
- **Problema:** la conexión dinámica del suministro de energía está activada, pero ninguno de los suministros de energía se muestra en el modo **En espera**.

- **Resolución A:** no hay suficiente alimentación excedente. Uno o más suministros de energía pasarán al estado En espera solo cuando el excedente de alimentación disponible en el gabinete supere la capacidad de al menos un suministro de energía.
- **Solución B:** la conexión dinámica de suministros de energía no es totalmente compatible con las unidades de suministro de energía presentes en el gabinete. Para verificar si es así, utilice la interfaz web para desactivar la conexión dinámica de suministros de energía y luego volver a encenderla. Si la conexión dinámica de suministros de energía no es totalmente compatible, aparecerá un mensaje.

- **Problema:** se insertó un nuevo servidor en el gabinete con suficientes suministros de energía, pero el servidor no se enciende.
  - **Solución A:** revise la configuración del límite de alimentación de entrada del sistema; es posible que la configuración sea demasiado baja para permitir que se enciendan los servidores adicionales.
  - **Solución B:** compruebe la configuración de conservación máxima de alimentación. Si está establecida, se presenta este problema. Para obtener más información, consulte los valores de configuración de la alimentación.
  - **Solución C:** compruebe la prioridad de alimentación de la ranura asociada con el servidor recién insertado y asegúrese de que no esté por debajo de cualquier otra prioridad de alimentación de ranura del servidor.
- **Problema:** la alimentación disponible cambia continuamente, aun cuando no haya cambiado la configuración de gabinete modular.
  - **Solución:** la CMC cuenta con administración dinámica de alimentación de ventiladores que reduce brevemente la asignación de alimentación a los servidores si el gabinete está funcionando cerca del límite máximo de alimentación configurado por el usuario; esto hace que se asigne alimentación a los ventiladores mediante la reducción del rendimiento del servidor para mantener el consumo de alimentación de entrada por debajo del **Límite de alimentación de entrada del sistema**. Este comportamiento es normal.
- **Problema:** se registraron <número> vatios como **Excedente para rendimiento pico.**
  - **Solución:** el gabinete tiene <número> vatios de alimentación excedente disponible en la configuración actual y el **Límite de alimentación de entrada del sistema** puede ser reducido de forma segura a esta cantidad sin afectar el rendimiento del servidor.
- **Problema:** un subconjunto de servidores perdió alimentación después de una falla en la red de CA, aun cuando el chasis estaba operando en la configuración de **Redundancia de cuadrícula** con cuatro suministros de energía.
  - **Resolución:** esto puede ocurrir si los suministros de energía se conectan incorrectamente a redes de CA redundantes en el momento en que ocurre la falla de la red de CA. La política de **Redundancia de la red eléctrica** requiere que los dos suministros de alimentación de la izquierda se conecten a una red de CA y los dos suministros de alimentación de la derecha se conecten a otra. Si dos unidades de suministro de energía están conectadas en forma incorrecta, por ejemplo, si PSU 2 y PSU 3 están conectadas a las redes de CA equivocadas, una falla en la red de CA ocasionará la pérdida de alimentación en los servidores de menor prioridad.
- **Problema:** los servidores de menor prioridad perdieron alimentación después de una falla en una unidad de suministro de energía.
  - **Solución:** para evitar que una falla futura en el suministro de energía ocasione que se apaguen los servidores, asegúrese de que el chasis tenga como mínimo tres suministros de energía y se configure de manera que la política de **Redundancia de suministro de energía** impida que la falla de una unidad de suministro de energía afecte la operación del servidor.
- **Problema:** el rendimiento general del servidor disminuye cuando aumenta la temperatura ambiente en el centro de datos.
  - **Solución:** esto puede ocurrir si el **Límite de alimentación de entrada del sistema** se configuró con un valor que provoca que una necesidad de alimentación mayor de los ventiladores se tenga que compensar con una reducción de alimentación para los servidores. El usuario puede aumentar el **Límite de alimentación de entrada del sistema** a un valor mayor de modo que se permita la asignación de alimentación adicional a los ventiladores sin afectar el rendimiento del servidor.

Solución de problemas de alertas

Use el registro de la CMC y el registro de rastreo para solucionar problemas con las alertas de la CMC. El éxito o la falla de cada intento de entrega de las capturas de SNMP o de correo electrónico se anota en el registro de la CMC. En el registro de rastreo se incluye información adicional que describe el error específico. Sin embargo, dado que SNMP no confirma la entrega de capturas, utilice un analizador de red o una herramienta como snmputil de Microsoft para rastrear los paquetes en el sistema administrado.

Visualización de los registros de sucesos

Es posible ver los registros de hardware y del chasis para obtener información sobre los sucesos críticos del sistema que se producen en el sistema administrado.

Visualización del registro de hardware

La CMC genera un registro de sucesos de hardware que ocurren en el chasis. Para ver el registro de hardware, utilice la interfaz web y RACADM remoto.

NOTA: Para borrar el registro de hardware, debe tener privilegios de Administrador de borrado de registros.

NOTA: Puede configurar la CMC para enviar capturas SNMP o correos electrónicos cuando ocurran sucesos específicos. Para obtener información sobre la configuración de la CMC para enviar alertas, consulte Configuración de la CMC para enviar alertas.

Ejemplos de anotaciones en el registro de hardware

```
critical System Software event: redundancy lost
Wed May 09 15:26:28 2007 normal System Software
event: log cleared was asserted
Wed May 09 16:06:00 2007 warning System Software
event: predictive failure was asserted
Wed May 09 15:26:31 2007 critical System Software
event: log full was asserted
Wed May 09 15:47:23 2007 unknown System Software
event: unknown event
```

Visualización de los registros de hardware mediante la interfaz web del CMC

Es posible ver, guardar y eliminar el registro de hardware. También es posible ordenar las entradas del registro según la gravedad, fecha y hora o la descripción al hacer clic en el encabezado de la columna. Si se vuelve a hacer clic en el encabezado de la columna se invertirá el orden.

Para ver los registros de hardware mediante la interfaz web de la CMC, en el panel izquierdo, haga clic en **Descripción general del chasis** > **Registros**. Aparecerá la página **Registro de hardware**. Para guardar una copia del registro de hardware en su red o Managed Station, haga clic en **Guardar registro** y luego especifique una ubicación para el archivo de texto del registro.

NOTA: Debido a que el registro se guarda como archivo de texto, no aparecerán en él las imágenes que se usan para indicar la gravedad en la interfaz del usuario. En el archivo de texto, la gravedad se indica con las palabras En buen estado, Informativo, Desconocido, Advertencia y Grave. Las entradas de fecha y hora aparecen en orden ascendente. Si <SYSTEM BOOT> aparece en la columna Fecha/Hora, significa que el suceso ocurrió durante el apagado o el encendido de alguno de los dispositivos, cuando no había fecha ni hora disponible.

Para borrar el registro de hardware, haga clic en **Borrar registro**.

NOTA: El CMC crea una nueva anotación de registro para indicar que el registro se borró.

NOTA: Para borrar el registro de hardware, debe tener privilegios de Administrador de borrado de registros.

Visualización de los registros de hardware mediante RACADM

Para ver el registro de hardware mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getsel
```

Para borrar el registro de hardware, escriba:

```
racadm clrsel
```

Visualización del registro del chasis

El CMC genera un registro de los sucesos relacionados con el chasis. La CMC proporciona capacidades de alerta a través del Registro de sucesos del sistema (SEL), SNMP y las interfaces de correo electrónico.

SPERC está insertada mientras uno o más servidores PowerEdge sirve están encendidos.

NOTA:

- Para borrar el registro del chasis, debe tener privilegios de **Administrador de borrado de registros**.

Visualización de los registros del chasis mediante RACADM

Para ver la información del registro del chasis mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba lo siguiente:

```
racadm chassislog view
```

Este comando muestra las últimas 25 entradas del registro del chasis.

Para ver las opciones de visualización de chassislogs disponibles, ejecute el siguiente comando:

```
racadm chassislog help view
```

Visualización de los registros del chasis mediante la interfaz web

Puede ver, guardar y borrar el registro del chasis. Puede filtrar los registros en función del tipo de registro y filtro. Además, puede realizar una búsqueda en función de una palabra clave o ver los registros en los días especificados.

En el panel izquierdo, haga clic en **Descripción general del chasis** > **Registros** > **Registros del chasis**. Aparecerá la página **Registro del chasis**.

Para guardar una copia del registro del chasis en la red o Managed Station, haga clic en **Guardar registro** y luego especifique una ubicación donde guardar el archivo del registro.

Uso de la consola de diagnósticos

Puede diagnosticar los problemas relacionados con el hardware del chasis mediante los comandos de CLI si es un usuario avanzado o un usuario bajo la dirección de asistencia técnica.

NOTA: Para modificar esta configuración, debe tener privilegios de Administrador de comandos de depuración.

Para acceder a la consola de diagnósticos:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Solución de problemas** > **Diagnósticos**.
   Aparecerá la página **Consola de diagnósticos**.
2. En el cuadro de texto **Comando**, escriba un comando y haga clic en **Enviar**.
   Para obtener información acerca de los comandos, consulte la *ayuda en línea*.

   Aparece la página de resultados del diagnóstico.

Restablecimiento de componentes

Es posible restablecer la CMC activa o volver a restablecer virtualmente los servidores de modo tal que se comporten como si se los hubiese quitado y vuelto a insertar. Si el chasis tiene un CMC en espera, el restablecimiento del CMC activo ocasiona una protección contra fallas y el CMC en espera se torna activo.

NOTA: Para restablecer componentes, debe tener privilegios de Administrador de comandos de depuración.

Para restablecer los componentes mediante la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Solución de problemas** > **Restablecer componentes**.

Aparecerá la página **Restablecer componentes**.

2 Para restablecer la CMC activa, en la sección **Estado de la CMC**, haga clic en **Reinicio/Conmutación por error de la CMC**. Si hay una CMC en espera y un chasis está completamente redundante, se produce una conmutación por error que hará que la CMC en espera se vuelva activa. Sin embargo, si no hay ninguna CMC en espera, la CMC disponible se reinicia.

3 Para volver a colocar de forma virtual el servidor, en la sección **Recolocación virtual de servidores**, seleccione los servidores que recolocará y haga clic en **Aplicar selecciones**.

Para obtener más información, consulte la *Ayuda en línea*.

Esta operación hace que los servidores se comporten como si se hubiesen quitado e insertado nuevamente.

Guardar o restaurar la configuración del chasis

Esta es una función con licencia. Para guardar o restaurar una copia de seguridad de la configuración del chasis mediante la interfaz web del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Configuración** > **Copia de seguridad del Chasis**. Aparecerá la página **Copia de seguridad del chasis**. Para guardar la configuración del chasis, haga clic en **Guardar**. Modifique la ruta de acceso del archivo predeterminado (opcional) y haga clic en **Aceptar** para guardar el archivo. El nombre del archivo de copia de seguridad predeterminado contiene la etiqueta de servicio del chasis. Este archivo de copia de seguridad se puede usar posteriormente para restaurar la configuración y los certificados para este chasis solamente.

2 Para restaurar la configuración del chasis, en la sección "Restaurar", haga clic en **Examinar**, especifique el archivo de copia de seguridad y, a continuación, haga clic en **Restaurar**.

NOTA:

- CMC no se reinicia al restaurar la configuración; sin embargo, es posible que se requiera algo de tiempo para que los servicios de la CMC asimilen los cambios o la nueva configuración. Una vez que el proceso se complete correctamente, se cerrarán todas las sesiones actuales.
- La información de Flexaddress, perfiles de servidor y almacenamiento extendido no se guardan ni se restauran con la configuración del chasis.

Solución de errores de protocolo de hora de red

Después de configurar la CMC de modo que el reloj esté sincronizado con un servidor de hora remota en la red, pueden transcurrir de 2 a 3 minutos hasta que se produzca un cambio en la fecha y hora. Si transcurrido este tiempo no se produce ningún cambio, puede ser necesario solucionar algún problema. Puede que la CMC no consiga sincronizar el reloj por alguna de las siguientes razones:

- Es posible que haya un problema con los valores de Servidor NTP (Protocolo de hora de la red) 1, Servidor NTP 2 y Servidor NTP 3.
- Es posible que se haya introducido accidentalmente un nombre de host o una dirección IP no válidos.
- Es posible que haya un problema de conectividad de red que impida que el CMC se comunique con alguno de los servidores NTP configurados.
- Podría existir un problema de DNS que impida que se resuelvan algunos nombres de host del servidor NTP.

Para solucionar los problemas relacionados con el NTP, revise la información del registro de rastreo de la CMC. Este registro contiene un mensaje de error para las fallas relacionadas con NTP. Si la CMC no puede sincronizarse con los servidores NTP remotos configurados, la hora de la CMC se sincronizará con el reloj del sistema local y el registro de rastreo incluirá una entrada similar a la siguiente:

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

También se puede verificar el estado de ntpd escribiendo el siguiente comando de racadm:

```
racadm getractime –n
```

La salida de este comando contiene estadísticas de NTP detalladas que pueden ser útiles para depurar el problema.

Si intenta configurar un servidor NTP basado en Windows, puede ser de utilidad aumentar el parámetro `MaxDist` para `ntpd`. Antes de cambiar este parámetro, entienda todas sus consecuencias, ya que el valor predeterminado debe ser lo suficientemente elevado para que funcione con la mayoría de los servidores NTP.

Para modificar el parámetro, escriba el comando siguiente:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

Después de realizar el cambio, desactive el NTP, espere entre 5 y 10 segundos y active el NTP nuevamente:

NOTA: NTP puede tardar 3 minutos más para sincronizarse nuevamente.

Para desactivar el NTP, escriba:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

Para activar el NTP, escriba:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

Si los servidores NTP se configuraron correctamente y esta anotación está presente en el registro de rastreo, se confirmará que el CMC no puede sincronizarse con ninguno de los servidores NTP configurados.

Si no está configurada la dirección IP del servidor NTP, posiblemente verá una anotación del registro de rastreo similar a:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address 1.2.3.4 Jan 8
19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Si se configuró un valor del servidor NTP con un nombre de host no válido, posiblemente verá una anotación del registro de rastreo similar a:

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21 14:34:27 cmc
ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

Para obtener información acerca de cómo especificar el comando `gettracelog` para revisar el registro de rastreo mediante la interfaz web de la CMC, consulte Using Diagnostic Console (Uso de la consola de diagnóstico).

Interpretación de los colores y los patrones de parpadeo de los LED

Los LED en el chasis proporcionan el siguiente estado de un componente:

- Los LED que se mantienen encendidos en color verde indican que el componente está encendido. Si el LED verde está parpadeando, indica un suceso crítico pero de rutina, por ejemplo una carga de firmware, durante el cual la unidad no está operativa. Este estado no indica una falla.
- Los LED que parpadean en color ámbar en un módulo indican una falla en ese módulo.
- Los LED que parpadean en color azul pueden ser configurados por el usuario y utilizados para la identificación. Para obtener más información acerca de la configuración, consulte Configuración de los LED para identificar componentes en el chasis.

Tabla 43. Colores y patrones de parpadeo de los LED

Componente	Color de LED, patrón de parpadeo	Estado
CMC	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Activo
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Modo de espera
Servidor	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas
Módulo de E/S (común)	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal/maestro de apilamiento
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas/esclavo de apilamiento
Módulo de E/S (de paso)	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	No se utiliza
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas
Ventilación	Verde, encendido permanentemente	Ventilador funcionando
	Verde, parpadeante	No se utiliza

Componente	Color de LED, patrón de parpadeo	Estado
	Verde, apagado	Apagado
	Ámbar, encendido permanentemente	Tipo de ventilador no reconocido, actualizar el firmware del CMC
	Ámbar, parpadeante	Falla del ventilador; tacómetro fuera de rango
	Ámbar, apagado	No se utiliza
PSU	(Ovalado) Verde, encendido permanentemente	CA en buen estado
	(Ovalado) Verde, parpadeante	No se utiliza
	(Ovalado) Verde, apagado	CA en mal estado
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Ámbar, apagado	Sin fallas
	(Circular) Verde, encendido permanentemente	CC en buen estado
	(Circular) Verde, apagado	CC en mal estado
Gabinete	Azul	Cuando el servidor host está identificando el gabinete
	Ámbar	Encendido o Restablecer, estado de error

Solución de problemas de un CMC que no responde

Si no puede iniciar sesión en el CMC por medio de ninguna de las interfaces (interfaz web, Telnet, SSH, RACADM remoto o serie), puede verificar la funcionalidad del CMC mediante la observación de sus indicadores LED en CMC, la obtención de información de recuperación con el puerto serie DB-9 o la recuperación de la imagen del firmware del CMC.

NOTA: No es posible iniciar sesión en el CMC en espera por medio de una consola serie.

Observación de los LED para aislar el problema

Hay dos indicadores LED en el lado izquierdo de la tarjeta:

- LED superior izquierda: indica el estado de alimentación. Si no está ENCENDIDO:
  - Verifique que haya corriente alterna presente en al menos un suministro de energía.
  - Asegúrese de que la tarjeta CMC esté instalada correctamente. Puede liberar o tirar de la palanca de expulsión, extraer la CMC y volver a instalarla asegurándose de que la placa esté insertada completamente y el seguro cierre correctamente.
- LED inferior izquierda: esta LED es de varios colores. Cuando la CMC está activa y en funcionamiento, y no hay ningún problema, la LED inferior es azul. Si es de color ámbar, se ha detectado una falla. La falla podría producirse por cualquiera de los siguientes tres sucesos:
  - Una falla del núcleo. En este caso, se debe reemplazar la placa de la CMC.
  - Una falla de autoprueba. En este caso, se debe reemplazar la placa de la CMC.
  - Una imagen dañada. En este caso, cargue la imagen de firmware de la CMC para recuperar la CMC.

NOTA: Un inicio o restablecimiento normal de la CMC demora un poco más de un minuto para iniciar su sistema operativo completamente y quedar disponible para el inicio de sesión. El indicador LED azul está activado en la CMC activa. En una configuración redundante con dos CMC, solo la LED verde de la parte superior derecha está activada en la CMC en espera.

Obtención de la información de recuperación desde el puerto serie DB-9

Si el LED inferior es de color ámbar, la información de recuperación está disponible en el puerto serie DB-9, que se ubica en el frente del CMC.

Para obtener la información de recuperación:

1 Instale un cable de módem NULO entre el sistema CMC y el sistema cliente.

2 Abra el emulador de terminal de su elección (como ser, HyperTerminal o Minicom). Cuando aparezca la petición, configure las siguientes especificaciones: 8 bits, sin paridad, sin control de flujo, tasa en baudios 115200.

3 Presione la tecla <Enter>.

Si aparece una petición de recuperación, habrá información adicional disponible. La petición indica el número de ranura de la CMC y el tipo de falla.

Para ver el motivo de la falla y la sintaxis para algunos comandos, escriba `recover` y presione <Enter>.

Peticiones de ejemplo:

```
recover1[self test] CMC 1 self test failure
```

```
recover2[Bad FW images] CMC2 has corrupted images
```

- Si la petición indica una falla de autoprueba, no habrá componentes utilizables en la CMC. La CMC está dañada y se debe regresar a Dell.
- Si la petición indica **Imagen del firmware dañada**, complete las tareas en la Recuperación de imagen del firmware.

Recuperación de la imagen del firmware

La CMC entra en el modo de recuperación cuando no es posible realizar un inicio normal del sistema operativo de la CMC. En el modo de recuperación, hay un pequeño subconjunto de comandos disponible que le permite reprogramar los dispositivos flash mediante la carga del archivo de actualización del firmware, **vrtx_cmc.bin**. Este es el mismo archivo de imagen del firmware que se utiliza para las actualizaciones normales del firmware. El proceso de recuperación muestra su actividad actual y se inicia en el sistema operativo de la CMC una vez que se completa.

Cuando escribe recuperación y luego presiona <Enter> en la petición de recuperación, aparece el motivo de la recuperación y los subcomandos disponibles. Un ejemplo de secuencia de recuperación podría ser:

```
recover getniccfg
recover setniccfg 192.168.0.120 255.255.255.0
192.168.0.1
recover ping 192.168.0.100
recover fwupdate -g -a 192.168.0.100
```

NOTA: Conecte el cable de red al conector RJ45 del extremo izquierdo.

NOTA: En el modo de recuperación, normalmente no puede enviar comandos ping a la CMC porque no hay ningún apilamiento de red activo. El comando `recover ping <TFTP server IP>` le permite enviar comandos ping al servidor TFTP para verificar la conexión LAN. Es posible que necesite utilizar el comando `recover reset` después de `setniccfg` en algunos sistemas.

Solución de problemas de red

El registro de rastreo integrado de la CMC permite depurar los sistemas de alerta y de red de la CMC. Es posible acceder al registro de rastreo mediante la interfaz web de la CMC o RACADM. Consulte la sección del comando `gettracelog` en *Chassis Management*

Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

El registro de rastreo da seguimiento a la siguiente información:

- DHCP: rastrea los paquetes que se envían a un servidor DHCP y que se reciben de él.
- DDNS: rastrea solicitudes y respuestas de actualización de DNS dinámico.
- Cambios de configuración en las interfaces de red.

El registro de rastreo también puede contener códigos de error específicos del firmware de la CMC que están relacionados con el firmware integrado de la CMC, no con el sistema operativo del sistema administrado.

Solución de problemas de la controladora

Para solucionar los problemas de una controladora:

1 En el panel izquierdo, haga clic en **Descripción general del chasis** > **Almacenamiento** > **Controladoras** > **Solución de problemas**.

2 En la página **Solución de problemas de la controladora**, vaya a la lista desplegable **Acciones** de la controladora correspondiente, seleccione cualquiera de las siguientes opciones y haga clic en **Aplicar**.

- **Restablecer configuración**: elimina los discos virtuales y las reservas activas. Sin embargo, no se borran los datos de los discos.

  NOTA: Al restablecer la configuración de PERC se descarta la caché fijada, si la hubiera, en la controladora PERC.

- **Exportar registro TTY**: se exporta el registro de depuración TTY de la controladora de almacenamiento al sistema local.
- **Descartar memoria caché anclada**: elimina los datos que están almacenados en la caché de la controladora RAID.

  NOTA: Si hay una caché anclada, aparece la opción para borrarla. Si no hay una caché anclada, esta opción no se muestra.

- **Desactivar controladora RAID**: desactiva la controladora homóloga. Esta opción está disponible en el menú desplegable solo para la PERC8 compartida (integrada 2) y las PERC8 compartidas externas.
- **Activar controladora RAID**: activa la controladora homóloga. La opción **Activar controladora RAID** está disponible en el menú desplegable.

  NOTA:

  Para una PERC desactivada, ninguna de las demás opciones Restablecer configuración, Exportar registro de TTY, Descartar caché anclada y Desactivar controladora RAID están disponibles en el menú desplegable.

- **Activar tolerancia a errores**: activa el modo de tolerancia a errores de la tarjeta PERC 8 compartida externa.
- **Desactivar tolerancia a errores**: desactiva el modo de tolerancia a errores de la tarjeta PERC 8 compartida externa.

  NOTA: Activar tolerancia a errores y Desactivar tolerancia a errores aparecen solo para las tarjetas PERC 8 compartidas externas. El modo predeterminado de la PERC 8 compartida externa es el modo sin tolerancia a errores.

NOTA:

- Muestra un mensaje de error si los servidores blade están encendidos.
- El comando no funciona si el servidor blade está encendido.

Acoplamiento activo de gabinetes en chasis con tolerancia a errores

1 Asegúrese de que las ranuras 5 y 6 del chasis no tengan tolerancia a errores.

2 Desconecte los gabinetes.

3 Cambie el estado de las ranuras 5 y 6 al modo de tolerancia a errores.

4 Vuelva a conectar los gabinetes en las conexiones de cables con tolerancia a errores.

Realice un ciclo de encendido del chasis después de desconectar los gabinetes y antes de volver a conectarlos, ya que las unidades conservan la reserva anterior SCSI-3 hasta que se realiza un ciclo de encendido en el chasis.

18

Uso de la interfaz del panel LCD

El panel LCD del chasis puede utilizarse para realizar tareas de configuración y diagnóstico, y para obtener información de estado acerca del chasis y su contenido.

En la siguiente figura se ilustra el panel LCD. La pantalla LCD muestra los menús, los íconos, las imágenes y los mensajes.

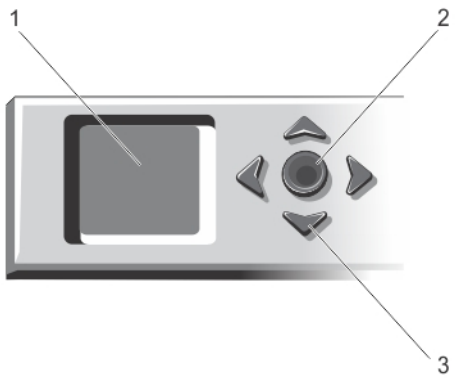


Figura 4. Pantalla LCD

1	Pantalla LCD	2	Botón de selección ("check")
3	Botones de desplazamiento (4)		

Temas:

Navegación de la pantalla LCD

El lado derecho del panel LCD tiene cinco botones: cuatro botones de flecha (arriba, abajo, izquierda y derecha) y un botón central.

- *Para desplazarse por las pantallas, use los botones de flecha derecha (siguiente) e izquierda (anterior). Mientras se usa el panel, es posible regresar a una pantalla anterior en cualquier momento.*
- *Para desplazarse a través de las opciones en una pantalla, utilice los botones de flecha hacia abajo y arriba.*
- *Para seleccionar y guardar un elemento en una pantalla y avanzar a la siguiente pantalla, utilice el botón central.*

Los botones de flecha hacia arriba, abajo, izquierda y derecha cambian los elementos o íconos del menú seleccionados en la pantalla. El elemento seleccionado se muestra con un fondo o borde celeste.

Si la longitud de los mensajes que se muestran en la pantalla LCD excede la capacidad de la pantalla, utilice los botones de flecha hacia la izquierda y la derecha para desplazarse por el texto en esas direcciones.

Los iconos que se describen en la tabla siguiente se usan para navegar por las pantallas LCD.

Tabla 44. Iconos de navegación del panel LCD

Icono normal	Icono resaltado	Nombre y descripción del icono
		**Atrás**: seleccione y presione el botón central para regresar a la pantalla anterior.
		**Aceptar/Sí**: seleccione y presione el botón central para aceptar un cambio y regresar a la pantalla anterior.
		**Omitir/Siguiente**: seleccione y presione el botón central para omitir los cambios y avanzar a la siguiente pantalla.
		**No**: seleccione y presione el botón central para responder "No" a una pregunta y avanzar a la siguiente pantalla.
		**Identificación del componente**: parpadea el LED azul en un componente. **NOTA: Se muestra un rectángulo azul parpadeante cerca de este icono cuando se activa la opción Identificación del componente.**

El LED indicador de estado en el panel LCD indica la condición general del chasis y de sus componentes.

- Azul continuo indica que está en buenas condiciones.
- Parpadeo en color ámbar indica que al menos un componente tiene una condición de falla.
- Parpadeo en color azul es una señal de identificación que se utiliza para identificar un chasis en un grupo de chasis.

Menú principal

Desde **Menú principal**, es posible navegar a una de las siguientes pantallas:

- **Asignación de KVM (Keyboard, video and mouse)**: contiene las opciones para asignar o desasignar KVM a los servidores.
- **Asignación de DVD**: esta opción aparece en la pantalla del **Menú principal** únicamente si hay una unidad de DVD instalada.
- **Gabinete**: muestra la información de estado del chasis.
- **Resumen de IP**: muestra información sobre CMC IPv4, CMC IPv6, iDRAC IPv4 e iDRAC 4 IPv6.
- **Configuración**: contiene opciones como **Idioma del LCD**, **Orientación del chasis**, **Pantalla LCD predeterminada** y **Configuración de la red**.

Menú de asignación de KVM

Desde esta pantalla puede ver la KVM para la información de asignación del servidor, asignar otro servidor para la KVM o desasignar la conexión existente. Para usar el KVM para un servidor, seleccione **Asignación de KVM** en el menú principal, navegue hasta el servidor correspondiente y, a continuación, presione el botón central **Verificación**.

Asignación de DVD

Al explorar esta página, puede ver el DVD para la información de asignación del servidor, asignar otro servidor a la unidad de DVD en el chasis o desasignar la conexión existente. Para que el servidor tenga acceso a la unidad de DVD, seleccione **Asignación de DVD** en el menú principal, navegue hasta el servidor requerido y, a continuación, presione el botón central de **Verificación**.

Es posible asignar la unidad de DVD a la ranura del servidor solamente si dicha unidad se encuentra activada para esa ranura del servidor. También se puede anular la asignación de la unidad de DVD para evitar que se utilice en las ranuras del servidor. Si el cable SATA no se conecta correctamente entre la unidad de DVD y la placa principal, la condición de la unidad de DVD será crítica. Si la condición de la unidad de DVD es crítica, el servidor no puede acceder a ella.

NOTA: La función Asignación de DVD aparece en la pantalla Menú principal del LCD solo si hay una unidad de DVD instalada.

Menú del alojamiento

Esta pantalla permite obtener acceso a las siguientes pantallas:

- **Estado de la parte delantera**
- **Estado de la parte posterior**
- **Estado de la parte lateral**
- **Estado del gabinete**

Use los botones de navegación para seleccionar el elemento correspondiente (seleccione el ícono **Atrás** para regresar al **Menú principal**) y presione el botón central. Aparecerá la pantalla seleccionada.

Menú Resumen de IP

La pantalla **Resumen de IP** muestra la información de IP del CMC (IPv4 y IPv6) y de cada servidor que está instalado en el chasis.

Use los botones de flecha hacia arriba y abajo para desplazarse por la lista. Use las flechas hacia la izquierda y hacia la derecha para desplazarse por los mensajes seleccionados que no caben en la pantalla.

Use los botones de flechas hacia arriba y hacia abajo para seleccionar el icono **Atrás** y presione el botón central para regresar al menú **Gabinete**.

Configuración

El menú **Configuración** muestra diversos elementos que pueden configurarse:

- **Idioma del LCD**: seleccione el idioma que desea utilizar para el texto y los mensajes de la pantalla LCD.
- **Orientación del chasis**: seleccione la opción **Modo torre** o bien **Modo bastidor** según la orientación del chasis durante la instalación.
- **Pantalla LCD predeterminada**: seleccione la pantalla (**Menú principal**, **Estado de la parte delantera**, **Estado de la parte posterior**, **Estado de la parte lateral** o **Personalizado**) que aparece cuando no hay actividad en el panel LCD.
- **Configuración de red**: seleccione esta opción para configurar los valores de red de una CMC. Para obtener más información acerca de esta función, consulte Configuración de la red de CMC mediante la interfaz del panel LCD.

Utilice los botones de flecha hacia arriba y abajo para resaltar una opción del menú o seleccione el icono **Atrás** si desea regresar al **Menú principal**.

Para activar la selección, presione el botón del centro.

Idioma de LCD

La pantalla **Idioma de LCD** le permite seleccionar el idioma usado para los mensajes del panel LCD. El idioma actualmente activo está resaltado con un fondo celeste.

1 Use los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia la derecha para resaltar el idioma deseado.

2 Presione el botón central. Aparecerá el icono **Aceptar** resaltado.
3 Para confirmar el cambio, presione el botón central. Aparecerá el menú **Configuración de LCD**.

Pantalla predeterminada

La **Pantalla predeterminada** permite cambiar la pantalla que el panel LCD muestra cuando no hay ninguna actividad en el panel. La pantalla predeterminada de fábrica es el **Menú principal.** Puede elegir entre las siguientes opciones de pantalla:

- **Menú principal**
- **Estado frontal** (vista gráfica frontal del chasis)
- **Estado posterior** (vista gráfica posterior del chasis)
- **Estado lateral** (vista gráfica izquierda del chasis)
- **Personalizado** (logotipo de Dell con nombre del chasis)

La pantalla actualmente activa aparece resaltada en celeste.

1 Utilice los botones de flecha hacia arriba y abajo para resaltar la pantalla que desea definir como predeterminada.
2 Presione el botón central. El icono **Aceptar** quedará resaltado.
3 Presione el botón central nuevamente para confirmar el cambio. Aparecerá la **Pantalla predeterminada**.

Diagnóstico

El panel LCD permite diagnosticar problemas en cualquier servidor o módulo del chasis. Si hay un problema o se produjo una falla en el chasis, en cualquier servidor o en otro módulo del chasis, el indicador de estado del panel LCD parpadea en color ámbar. En el **Menú principal**, un ícono con fondo color ámbar aparece junto al ítem del menú (Gabinete) que conduce al estado frontal, trasero, lateral o de gabinete.

Al seguir los iconos color ámbar a través del sistema de menús de la pantalla LCD, es posible visualizar la pantalla de estado y los mensajes de error del elemento que presenta el problema.

Los mensajes de error del panel LCD pueden quitarse al eliminar el módulo o el servidor que causa el problema o borrar el registro de hardware del módulo o servidor. En el caso de errores del servidor, use la interfaz web o la interfaz de línea de comandos del iDRAC para borrar el registro de sucesos del sistema (SEL) del servidor. En el caso de errores del chasis, use la interfaz web o la interfaz de línea de comandos de la CMC para borrar el registro de hardware.

Mensajes de la pantalla LCD del panel frontal

Esta sección incluye dos apartados que muestran los mensajes de error y la información de estado que aparecen en la pantalla LCD del panel frontal.

Los *mensajes de error* de la pantalla LCD tienen un formato similar al del registro de sucesos del sistema (SEL) que se visualiza en la interfaz web o en CLI.

La tabla en la sección de errores muestra los mensajes de error y de advertencia que aparecen en las diferentes pantallas LCD y la causa posible de cada mensaje. El texto entre comillas angulares (< >) indica que el texto puede variar.

La *información de estado* en la pantalla LCD incluye información descriptiva sobre los módulos en el chasis. Las tablas en esta sección describen la información que se muestra para cada componente.

Información de estado del servidor y del módulo de LCD

En las tablas que figuran en esta sección se describen las opciones de estado que se muestran en la pantalla LCD del panel frontal para cada tipo de componente del chasis.

Tabla 45. Estado de la CMC

Elemento	Descripción
Nombre/Ubicación	Ejemplo: CMC1, CMC2
Sin errores	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Versión del firmware	Solo se muestra en una CMC activa Aparece el mensaje "en espera" para la CMC en espera
IP4 <activado, desactivado>	Muestra el estado actual activado de IPv4 únicamente en un CMC activo.
Dirección IP4: <dirección, adquiriendo>	Solo se muestra si IPv4 está activado únicamente en un CMC activo.
IP6 <activado, desactivado>	Muestra el estado actual activado de IPv6 únicamente en un CMC activo.
Dirección local IP6: <dirección>	Solo se muestra si IPv6 está activado únicamente en un CMC activo.
Dirección MAC	Muestra la dirección MAC del CMC.

Tabla 46. Estado del chasis o del gabinete

Elemento	Descripción
Nombre definido por el usuario	Ejemplo: "Sistema de bastidor Dell". Esto puede configurarse con la CLI del CMC o la interfaz web.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Número de modelo	Ejemplo: "PowerEdgeM1000".
Consumo de alimentación	Consumo de alimentación actual en vatios.
Alimentación pico	Consumo de alimentación pico en vatios.
Alimentación mínima	Consumo mínimo de alimentación en vatios.
Temperatura ambiente	Temperatura ambiente actual en grados Celsius.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.
Modo de redundancia del CMC	No redundante o Redundante.
Modo de redundancia de la unidad de suministro de energía	No redundante, Redundancia de cuadrícula o Redundancia de CC.

Tabla 47. Estado del ventilador

Elemento	Descripción
Nombre/Ubicación	Ejemplo: Fan1, Fan2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
RPM	Velocidad actual del ventilador en RPM.

Tabla 48. Estado de la unidad de suministro de energía

Elemento	Descripción
Nombre/Ubicación	Ejemplo: PSU1, PSU2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Estado	Desconectado, conectado o en espera: indica el estado de la alimentación de una unidad de suministro de energía.
Potencia máxima	Potencia máxima que la unidad de suministro de energía puede proporcionar al sistema.

Tabla 49. Estado del módulo de E/S

Elemento	Descripción
Nombre/Ubicación	Módulo de E/S A
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Estado	Apagado o encendido: indica si el M. E/S está funcionando.
Modelo	Modelo del módulo de E/S.
Tipo de red Fabric	Tipo de sistema de red.
dirección IP	Solo se muestra si los módulos de E/S están encendidos. En el tipo de módulo de E/S de paso el valor es cero.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.

Tabla 50. Estado de asignación de KVM

Elemento	Descripción
Servidor <número>	Muestra una lista de los servidores a los que se les puede asignar KVM.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Asignado	Muestra una lista de los servidores asignados a un KVM, si los hubiera.
Ranura <número>	Indica la ranura del servidor a la que el KVM está asignado. Los valores posibles son SLOT-*<01 a 04>*.
Desasignado	Se muestra si el KVM no está asignado a ninguno de los servidores.

Tabla 51. Estado de asignación de DVD

Elemento	Descripción
Servidor <número>	Muestra una lista de los servidores a los que se les puede asignar el DVD.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Asignado	Muestra una lista de los servidores asignados a un DVD, si los hubiera.
Ranura <número>	Indica la ranura del servidor a la que el DVD está asignado. Los valores posibles son SLOT-*<01 a 04>*.
Desasignado	Se muestra si el KVM no está asignado a ninguno de los servidores.

Tabla 52. Estado del ventilador

Elemento	Descripción
Nombre/Ubicación	Ejemplo: Blower1, Blower2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
RPM	Velocidad actual del ventilador en RPM.

Tabla 53. Estado de SPERC

Elemento	Descripción
SPERC: <número>	Muestra el nombre de SPERC en el formato SPERC n, donde 'n' es el número de SPERC. Ejemplo: SPERC 1, SPERC 2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Estado del trabajo	Activado o desactivado: indica si la SPERC está en funcionamiento.
Nombre: <nombre>	Nombre de Shared PERC. Ejemplo: SPERC
Estado de condición	En buen estado
Versión del firmware	Versión del SPERC
Fabricante	Nombre del fabricante
Estado	Desconectado, conectado o en espera: indica el estado de alimentación de un SPERC.

Tabla 54. Estado de la tarjeta PCIe

Elemento	Descripción
Tarjeta PCIe *<número>*	Muestra el nombre de la tarjeta PCIe en el formato Tarjeta PCIe *<n>*, donde "n" es el número de la tarjeta PCIe. Ejemplo: Tarjeta PCIe 1, Tarjeta PCIe 2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Estado del trabajo	Activado o desactivado: indica si la tarjeta PCIe está en funcionamiento.

Elemento	Descripción
Nombre: <nombre>	Nombre de la tarjeta PCIe.
Asignada a un servidor	Asignada o desasignada.

Tabla 55. Estado de la unidad de disco duro

Elemento	Descripción
Unidad de disco duro: <número>	Muestra el nombre de la unidad de disco duro en el formato de la unidad de disco duro <*n*>, donde 'n' es el número de la unidad de disco duro. Ejemplo: Unidad de disco duro 1, unidad de disco duro 2 y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos.
Estado de la alimentación	Rotación alta, transición, rotación baja: indica el estado de la alimentación de una unidad de disco duro
Fabricante	Nombre del fabricante
Capacidad	La capacidad de almacenamiento disponible de la unidad de disco duro en gigabytes (GB)
Versión del firmware	Muestra la versión del firmware de la unidad de disco duro
Estado	Desconectado, conectado o en espera: indica el estado de la alimentación de la unidad de disco duro.

Tabla 56. Server Status (Estado del servidor)

Elemento	Descripción
Nombre/Ubicación	Ejemplo: Servidor 1, Servidor 2, y así sucesivamente.
Sin errores	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos. Para obtener más información, consulte "Mensajes de error de la pantalla LCD".
Nombre de ranura	Nombre de ranura del chasis. Por ejemplo, SLOT-01. **NOTA: Puede configurar esta tabla a través de la CLI o la interfaz web del CMC.**
Nombre	Nombre del servidor, que el usuario puede establecer mediante Dell OpenManage. El nombre se muestra únicamente si el iDRAC completó el inicio y si el servidor admite esta función; de lo contrario, se muestran los mensajes de inicio del iDRAC.
Número de modelo	Se muestra si el iDRAC completó el inicio.
Etiqueta de servicio	Se muestra si el iDRAC completó el inicio.
Versión del BIOS	Versión del firmware del BIOS del servidor.
Último código de la POST	Muestra la cadena de mensajes del último código de la POST del BIOS del servidor.
Versión del firmware del iDRAC	Se muestra si el iDRAC completó el inicio. **NOTA: La versión del iDRAC 1.01 se muestra como 1.1. No hay versión 1.10 del iDRAC.**

Elemento	Descripción
IP4 <activado, desactivado>	Muestra el estado actual activado del IPv4.
Dirección IP4: <dirección, adquiriendo>	Solo se muestra si IPv4 está activado.
IP6 <activado, desactivado>	Solo se muestra si el iDRAC admite IPv6. Muestra el estado actual activado del IPv6.
Dirección local IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
Dirección global IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
FlexAddress activado en la red Fabric	Solo se muestra si la función está instalada. Enumera las redes Fabric activadas para dicho servidor (es decir, A, B, C).

La información de la tabla se actualiza de forma dinámica. Si el servidor no admite esta función, la siguiente información no aparecerá; de lo contrario, las opciones de Server Administrator son las siguientes:

- Opción “Ninguna” = No se debe mostrar ninguna cadena en la pantalla LCD.
- Opción “Predeterminada” = Ningún efecto.
- Opción “Personalizada” = Permite introducir un nombre de cadena para el servidor.

La información se muestra únicamente si el iDRAC completó el inicio. Para obtener más información sobre esta función, consulte la *RACADM Command Line Reference Guide for CMC in PowerEdge VRTX* (Guía de referencia de línea de comandos de RACADM para la CMC en PowerEdge VRTX).

19

Preguntas frecuentes

En esta sección se enumeran las preguntas frecuentes para los elementos siguientes:

- RACADM
- Administración y recuperación de un sistema remoto
- Active Directory
- FlexAddress y FlexAddressPlus
- Módulos de E/S

Temas:

RACADM

Después de restablecer el CMC (con el subcomando RACADM racreset), al introducir un comando, se muestra el siguiente mensaje:

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

¿Qué significa este mensaje?

Debe ejecutarse otro comando únicamente después de que el CMC termine de restablecerse.

Al usar subcomandos RACADM a veces se muestra uno o más de los siguientes errores:

- Mensajes de error locales: problemas de sintaxis, errores tipográficos, nombres incorrectos, etc. Por ejemplo, `ERROR: <message>`
  Use el subcomando `help` de RACADM para mostrar la sintaxis correcta y la información de uso. Por ejemplo, si se produce un error al borrar el registro del chasis, ejecute el siguiente subcomando:
  ```
  racadm chassislog help clear
  ```
- Mensajes de error relacionados con la CMC: problemas en los que la CMC no puede ejecutar una acción. Se muestra el siguiente mensaje de error:
  ```
  racadm command failed.
  ```

Para ver información sobre un chasis, escriba el siguiente comando:

```
racadm gettracelog
```

Durante el uso del RACADM del firmware, la petición cambia a ">" y la petición "$" ya no se muestra.

Si escribe un solo carácter de comillas dobles (") o simple (') sin el cierre correspondiente en el comando, la CLI cambiará a ">" y pondrá todos los comandos en cola.

Para regresar a la petición "$", presione <Ctrl>–d:

Se mostrará un mensaje de error `Not Found` mientras se utilizan los comandos `$ logout` y `$ quit`

Administración y recuperación de un sistema remoto

¿Por qué no están disponibles RACADM remoto y los servicios web después de un cambio de propiedad?

Es posible que los servicios de RACADM remoto y de la interfaz web tarden un minuto para estar disponibles después de que el componente Web Server de la CMC se restablece.

El Web Server de la CMC se restablece después de que se producen los siguientes acontecimientos:

- Se cambia la configuración de la red o las propiedades de seguridad de la red por medio de la interfaz de usuario web de la CMC.
- Se cambia la propiedad cfgRacTuneHttpsPort (incluso cuando un comando config -f <archivo de configuración> la cambia).
- Se utiliza `racresetcfg` o se restablece una copia de seguridad de la configuración del chasis.
- Se restablece la CMC.
- Se carga un nuevo certificado del servidor SSL.

¿Mi servidor DNS no registra mi CMC?

Algunos servidores DNS solo registran nombres de 31 caracteres como máximo.

Al obtener acceso a la interfaz web de la CMC, aparece una advertencia de seguridad que indica que el certificado SSL fue emitido por una autoridad de certificados que no es confiable.

La CMC incluye un certificado de servidor de CMC predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Este certificado no es emitido por una autoridad de certificados confiable. Para abordar este problema de seguridad, cargue un certificado de servidor de la CMC emitido por una autoridad de certificados confiable (por ejemplo, Thawte o Verisign).

¿Por qué se muestra el mensaje siguiente por motivos desconocidos?

Remote Access: SNMP Authentication Failure

Como parte de la detección, IT Assistant intenta verificar los nombres de comunidad **Obtener** y **Establecer** del dispositivo. En IT Assistant, el **nombre de comunidad Obtener = público** y el **nombre de comunidad Establecer = privado.** De manera predeterminada, el nombre de comunidad para el agente de CMC es "público". Cuando IT Assistant envía una solicitud establecer, el agente de CMC genera el error de autentificación SNMP porque solo acepta solicitudes de **comunidad = público.**

Cambie el nombre de comunidad de la CMC mediante RACADM. Para ver el nombre de comunidad de la CMC, utilice el siguiente comando:

```
racadm getconfig -g cfgOobSnmp
```

Para establecer el nombre de comunidad de la CMC, utilice el siguiente comando:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
```

Para evitar que se generen capturas de autentificación SNMP, debe ingresar nombres de comunidad que acepte el agente. Como la CMC solo permite un nombre de comunidad, debe introducir el mismo nombre de comunidad Obtener y Establecer para la configuración de detección de IT Assistant.

Al obtener acceso a la interfaz web de la CMC, se muestra una advertencia de seguridad que indica que el nombre de host del certificado SSL no coincide con el nombre de host de la CMC.

La CMC incluye un certificado de servidor de CMC predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Cuando se utiliza este certificado, el explorador web muestra una advertencia de seguridad si el certificado predeterminado no coincide con el nombre de host de la CMC (por ejemplo, la dirección IP).

Para solucionar este problema de seguridad, cargue un certificado de servidor de la CMC emitido a la dirección IP de la CMC. Al generar la solicitud de firma de certificado (CSR) que se utilizará para emitir el certificado, asegúrese de que el nombre común (CN) de la CSR tenga la misma dirección IP que la CMC (por ejemplo, 192.168.0.120) o el mismo nombre DNS registrado de la CMC.

Para asegurarse de que la CSR coincida con el nombre DNS registrado del CMC:

1 En el panel izquierdo, haga clic en **Descripción general del chasis.**
2 Haga clic en **Red**.
Aparecerá la página **Configuración de la red**.
3 Seleccione la opción **Registrar la CMC en DNS**.
4 Introduzca el nombre del CMC en el campo **Nombre de la CMC de DNS**.
5 Haga clic en **Aplicar cambios**.

Active Directory

¿Admite Active Directory el inicio de sesión en el CMC en varios árboles?

Sí. El algoritmo de consulta de Active Directory de la CMC admite varios árboles en un solo bosque.

¿El inicio de sesión en el CMC mediante Active Directory funciona en el modo mixto (es decir, los controladores de dominio del bosque ejecutan diferentes sistemas operativos, como Microsoft Windows 2000 o Windows Server 2003)?

Sí. En el modo mixto, todos los objetos utilizados por el proceso de consulta de la CMC (entre el usuario, el objeto del dispositivo del RAC y el objeto de asociación) tienen que estar en el mismo dominio.

El complemento Usuarios y equipos de Active Directory extendido por Dell verifica el modo y limita a los usuarios a fin de crear objetos en varios dominios si se encuentra en modo mixto.

¿El uso del CMC con Active Directory admite varios entornos de dominio?

Sí. El nivel de la función del bosque de dominios debe estar en el modo Nativo o en el modo Windows 2003. Asimismo, los grupos entre el objeto de asociación, los objetos de usuario de RAC y los objetos de dispositivo de RAC (incluido el objeto de asociación) deben estar en grupos universales.

¿Estos objetos extendidos por Dell (objeto de asociación Dell, dispositivo de RAC de Dell y objeto de privilegio Dell) pueden estar en dominios diferentes?

El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento Usuarios y equipos de Active Directory extendido por Dell permite crear estos dos objetos solamente en el mismo dominio. Otros objetos pueden estar en diferentes dominios.

¿Existe alguna restricción para la configuración del controlador de dominio de SSL?

Sí. Todos los certificados SSL para los servidores Active Directory que se encuentran en el bosque deben estar firmados mediante el mismo certificado con firma de la autoridad de certificados raíz, pues la CMC solo permite cargar un certificado SSL firmado por una autoridad de certificados de confianza.

La interfaz web no se inicia una vez que se creó y se cargó un nuevo certificado RAC.

Si se utilizan los servicios de certificados de Microsoft para generar el certificado RAC, es posible que se haya utilizado la opción Certificado de usuario en lugar de Certificado web durante la creación del certificado.

Para solucionar el problema, genere una CSR, cree un certificado web nuevo mediante el uso de los servicios de certificados de Microsoft y cárguelo por medio de ejecutar los siguientes comandos de RACADM:

```
racadm sslcsrgen [-g] [-f {filename}]

racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress y FlexAddressPlus

¿Qué sucede si se quita una tarjeta de función?

No existen cambios visibles si se quita una tarjeta de función. Este tipo de tarjetas pueden quitarse y almacenarse, o bien, pueden dejarse colocadas.

¿Qué sucede si se quita una tarjeta de función que se utilizó en un chasis y se coloca en otro?

La interfaz web muestra el siguiente mensaje de error:

```
This feature card was activated with a different chassis. It must be removed before accessing
the FlexAddress feature.

Current Chassis Service Tag = XXXXXXXX

Feature Card Chassis Service Tag = YYYYYYYY

An entry is added to the CMC log that states:

cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis ID='XXXXXXXX'
```

¿Qué sucede si se quita la tarjeta de función y se instala una tarjeta que no sea de FlexAddress?

No se debe activar ni modificar la tarjeta. La tarjeta es ignorada por la CMC. En esta situación, el comando **$racadm featurecard -s** muestra el siguiente mensaje:

```
No feature card inserted

ERROR: can't open file
```

Si se reprograma la etiqueta de servicio del chasis, ¿qué sucede si hay una tarjeta de función vinculada a ese chasis?

- Si la tarjeta de función original está presente en la CMC activo en ese chasis o cualquier otro, la interfaz web mostrará el siguiente error:
  - `This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.`
  - `Current Chassis Service Tag = XXXXXXXX`
  - `Feature Card Chassis Service Tag = YYYYYYYY`

  La tarjeta de función original ya no se puede seleccionar para desactivarla en ese chasis ni en ningún otro, salvo que el servicio de Dell vuelva a programar la etiqueta de servicio del chasis original en un chasis y que el CMC con la tarjeta de función original se active en ese chasis.
- La función FlexAddress continúa activada en el chasis vinculado originalmente. La vinculación de esa función del chasis se actualiza para reflejar la nueva etiqueta de servicio.

¿Se muestra un mensaje de error si hay dos tarjetas de función instaladas en el sistema de CMC redundante?

La tarjeta de función de la CMC activa se activó y está instalada en el chasis. La CMC ignora la segunda tarjeta.

¿La tarjeta SD tiene un dispositivo de protección contra escritura?

Sí. Antes de instalar la tarjeta SD en el módulo de CMC, verifique que el seguro de protección contra escritura esté desbloqueado. La función FlexAddress no podrá activarse si la tarjeta SD está protegida contra escritura. En esta situación, el comando **$racadm feature -s** muestra el siguiente mensaje:

```
No features active on the chassis. ERROR: read only file system
```

¿Qué sucede si no hay una tarjeta SD en el módulo CMC activo?

El comando **$racadm featurecard -s** muestra este mensaje:

```
No feature card inserted.
```

¿Qué le sucede a la función FlexAddress si el BIOS del servidor se actualiza de la versión 1.xx a la versión 2.xx?

Se debe apagar el módulo del servidor para poder usarlo con FlexAddress. Una vez completada la actualización del BIOS del servidor, el módulo del servidor no recibirá direcciones asignadas por el chasis hasta que se haya activado el ciclo de encendido del servidor.

¿Cómo se puede recuperar una tarjeta SD si no se encontraba en el chasis al ejecutar el comando de desactivación en FlexAddress?

El problema es que la tarjeta SD no puede utilizarse para instalar FlexAddress en otro chasis si no se encontraba en la CMC al momento de desactivar FlexAddress. Para recuperar el uso de la tarjeta, insértela de nuevo en una CMC del chasis al que esté vinculada, reinstale FlexAddress y luego desactive FlexAddress nuevamente.

La tarjeta SD está correctamente instalada, como así también todas las actualizaciones de firmware y software. La función FlexAddress está activa, pero la pantalla de implementación del servidor no muestra las opciones para implementarla. ¿Cuál es el problema?

Este es un problema de almacenamiento en caché del explorador. Cierre sesión en el explorador e inícielo nuevamente.

¿Qué sucede con FlexAddress si debo restablecer la configuración del chasis con el comando RACADM? racresetcfg?

La función FlexAddress permanecerá activada y disponible para su uso. Se seleccionan en forma predeterminada todas las ranuras y redes Fabric.

NOTA: Se recomienda especialmente apagar el chasis antes de ejecutar el comando RACADM `racresetcfg`.

Después de desactivar únicamente la función FlexAddressPlus (dejando FlexAddress activada), ¿por qué falla el comando racadm setflexaddr en la CMC (aún activa)?

Si el CMC posteriormente pasa a estar activo, y la tarjeta de función FlexAddressPlus está insertada en la ranura, la función FlexAddressPlus se reactiva y es posible reanudar los cambios de la configuración de FlexAddress para ranuras y redes Fabric.

Módulos de E/S

Después de realizar un cambio en la configuración, algunas veces, el CMC muestra la dirección IP 0.0.0.0.

Haga clic en el ícono **Actualizar** para ver si la dirección IP está configurada correctamente en el switch. Si se comete un error al configurar la dirección IP, la máscara o la puerta de enlace, el switch no configurará la dirección IP y mostrará 0.0.0.0 en todos los campos.

Errores comunes:

- Configurar la dirección IP fuera de banda con el mismo valor que la dirección IP de administración en banda o en la misma red que esta última.
- Introducir una máscara de subred no válida.
- Configurar la puerta de enlace predeterminada con una dirección que no está en una red directamente conectada al conmutador.