Dell Chassis Management Controller Version 2.21 for PowerEdge FX2 and FX2s

Guía del usuario

December 2019
Rev. A00

Notas, precauciones y advertencias

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

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

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

Tabla de contenido

1

Resumen

Dell Chassis Management Controller (CMC, Consola de administración del chasis) para Dell EMC PowerEdge FX2/FX2s es un hardware de administración de sistemas y una solución de software para administrar el chasis **PowerEdge FX2/FX2s**. La CMC cuenta con su propio microprocesador y memoria y recibe energía del chasis modular al que está conectado.

La 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 la información de asignación de PCIe y reasignar ranuras de PCIe.
- Proporcionar una interfaz de administración de uno a varios a los iDRAC y los módulos de E/S en el 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 notifica el consumo de energía en tiempo real, lo que incluye el registro de los puntos máximos y mínimos con una indicación de hora.
  - La 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.
  - La CMC supervisa y controla automáticamente las funciones de los ventiladores de enfriamiento en función de mediciones reales de la temperatura interna y ambiente.
  - La CMC proporciona informes completos de errores o de estado y del inventario del gabinete.
- La CMC proporciona un mecanismo para configurar de forma centralizada lo siguiente:
  - Los valores de red y seguridad del gabinete Dell PowerEdge FX2/FX2s.
  - 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. Además, la CMC desactiva componentes, de ser necesario, para proteger el hardware del sistema.
  - La seguridad de acceso de los usuarios.
  - Las ranuras de PCIe

Es posible configurar la 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.

NOTA: Los términos "sled de almacenamiento" y "módulo de almacenamiento" se usan de manera indistinta en este documento.

Temas:

- Otros documentos que puede necesitar
- Acceso a documentos desde el sitio de asistencia de Dell EMC

Funciones clave

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

Novedades de esta versión

Esta versión de la CMC para Dell EMC PowerEdge FX2/FX2s admite:

- Activación del cambio forzado de contraseña para cumplir con las regulaciones SB-327 de California, EE. UU.
- Regeneración de la clave autofirmada de SSH mediante el comando de la CLI.
- Actualización del paquete OpenSSH de código abierto a la versión 7.9p1.
- Actualización del paquete OpenSSH de código abierto a la versión 1.0.2r.

Funciones de administración

El CMC proporciona las siguientes funciones de administración:

- 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.
- Administración y supervisión remotas del sistema mediante SNMP, una interfaz web, KVM integrada, Telnet o una conexión de 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 varios componentes del chasis: permite actualizar el firmware para CMC, iDRAC en los servidores, sleds de almacenamiento e infraestructura del chasis.
- Actualización de firmware de componentes del servidor, como el BIOS y las controladoras de red 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.
- Adaptación del sled de varios nodos. PowerEdge FM120x4 es un sled de múltiples nodos.
- Supervisión de límite de alimentación del chasis.
- Compatibilidad de la función de identidad de E/S del iDRAC con el inventario mejorado de direcciones WWN/MAC.
- Función FlexAddress: reemplaza las identificaciones WWN/MAC (Nombre a nivel mundial/Control de acceso a medios) asignadas de fábrica por identificaciones WWN/MAC asignadas por el chasis para una ranura particular; se trata de una actualización opcional.
- Gráfico de la condición y el estado de los componentes del chasis.
- Asistencia para servidores simples o de varias ranuras.
- 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.
- Administración de múltiples chasis donde se permite que hasta diecinueve chasis sean visibles desde el chasis principal.

  NOTA: La administración de chasis múltiples no se admite en redes IPv6.
- Función de proxy de RACADM local y remoto del iDRAC para administrar sleds de almacenamiento en el chasis FX2s.

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 ID de usuario y contraseña 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.
- Imagen de la CMC firmada: se utiliza para proteger la imagen de firmware contra la modificación no detectada mediante la firma digital.

Descripción general del chasis

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

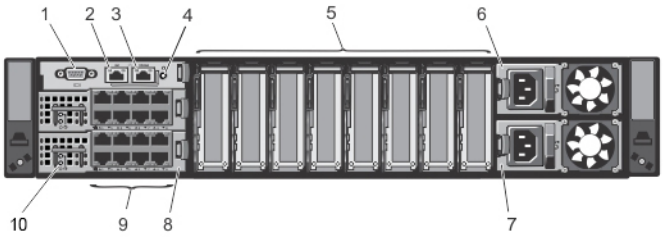


Ilustración 1. Panel posterior del chasis

Tabla 1. Panel posterior del chasis: componentes

Elemento	Indicador, botón o conector
1	Conector serie
2	Conector Ethernet Gb1
3	Conector Ethernet STK/GB2 (pila)
4	Botón de identificación del sistema
5	Ranuras de expansión PCIe de perfil bajo
6	Fuente de alimentación (PSU1)
7	Fuente de alimentación (PSU2)
8	Módulo de E/S (2)
9	Puertos del módulo de E/S

Tabla 1. Panel posterior del chasis: componentes (continuación)

Elemento	Indicador, botón o conector
10	Indicadores del módulo de E/S

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

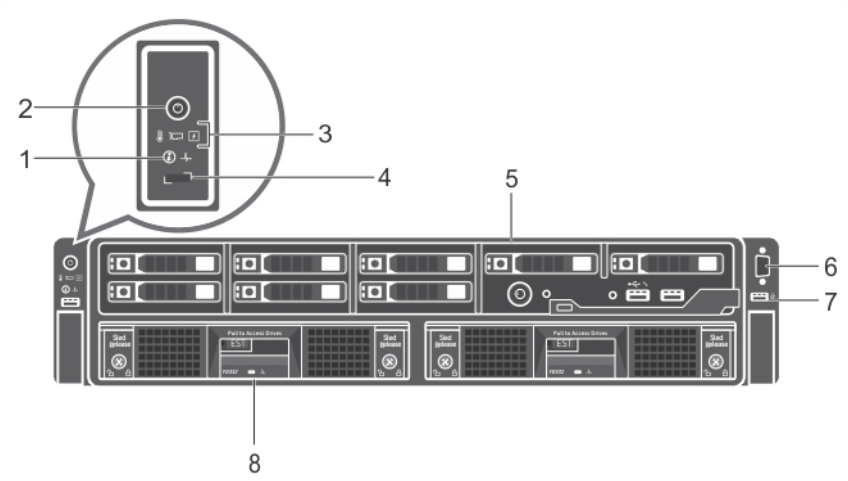


Ilustración 2. Panel frontal del chasis

Tabla 2. Panel frontal del chasis: componentes

Elemento	Indicador, botón o conector
1	Botón de identificación del sistema
2	Indicador de encendido, botón de encendido del gabinete
3	Indicadores de diagnóstico
4	Botón de selección de KVM
5	Sled de cómputo
6	Conector de vídeo
7	Conector USB
8	Sled de almacenamiento

Conexiones de acceso remoto admitidas

En la siguiente tabla se muestran las conexiones de acceso remoto admitidas.

Tabla 3. Conexiones de acceso remoto admitidas

Conexión	Funciones
Puertos de la interfaz de red de la CMC	• Puerto Gb: interfaz de red dedicada para la interfaz web de la CMC. La CMC tiene dos puertos RJ-45 Ethernet: ○ GB1 (puerto de vínculo ascendente) ○ Gb2 (puerto de consolidación de cables o apilamiento). El puerto STK/GB2 también se puede utilizar para la conmutación por error de NIC de la CMC.

Tabla 3. Conexiones de acceso remoto admitidas (continuación)

Conexión	Funciones
	NOTA: Asegúrese de que el valor de configuración predeterminado de la CMC se cambia del valor predeterminado **Apilamiento** a **Redundante** para implementar la conmutación por error de NIC. **PRECAUCIÓN: La conexión del puerto STK/Gb2 a la red de administración producirá resultados impredecibles si la configuración de la CMC no se ha cambiado del valor predeterminado Apilamiento a Redundante para implementar la conmutación por error de NIC. En el modo de apilamiento predeterminado, el cableado de los puertos Gb1 y STK/Gb2 a la misma red (dominio de difusión) puede producir una saturación por difusión. También se puede producir una saturación por difusión si la configuración de CMC se cambia al modo redundante, pero el cableado está conectado en cadena tipo margarita entre el chasis en el modo de apilamiento. Asegúrese de que el cableado modelo coincide con la configuración de CMC para el uso previsto.** • 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). • 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 intercambio binario para aplicaciones diseñadas específicamente 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).

Plataformas admitidas

La CMC admite los modelos de chasis **PowerEdge FX2** y **FX2s**. Las plataformas soportadas son PowerEdge FC430, PowerEdge FC630, PowerEdge FM120x4, PowerEdge FC830, PowerEdge FC640 y PowerEdge FD332. Para obtener información sobre la compatibilidad con la CMC, consulte la documentación de su dispositivo.

Para obtener información sobre las plataformas soportadas más recientes, consulte las *Notas de publicación de Dell Chassis Management Controller (CMC) versión 2.0 para Dell PowerEdge FX2/FX2s* disponibles en **dell.com/support/manuals**.

Navegadores web compatibles

Para obtener la información más reciente acerca de los navegadores web admitidos, consulte *Notas de la versión de Dell Chassis Management Controller (CMC) versión 2.1 para Dell PowerEdge FX2/FX2s* disponible en **dell.com/cmcmanuals**.

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari versión 10.1.2
- Safari versión 11.1.2
- Mozilla Firefox 61
- Mozilla Firefox 62
- Google Chrome 68
- Google Chrome 69

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+
```

Versiones de firmware admitidas

En la siguiente tabla se muestran las versiones de firmware de BIOS, iDRAC y Lifecycle Controller admitidas por los servidores mencionados:

Tabla 4. Versiones de firmware más recientes de BIOS, iDRAC y Lifecycle Controller

Servidores	BIOS	iDRAC	Lifecycle Controller
PowerEdge FC830	2.7.1	2.52.52.52	2.52.52.52
PowerEdge FC630	2.7.1	2.52.52.52	2.52.52.52
PowerEdge FC430	2.7.1	2.52.52.52	2.52.52.52
PowerEdge FM120	1.70	2.52.52.52	2.52.52.52
PowerEdge FC640	1.37	3.18.18.18	3.18.18.18

Versiones de firmware admitidas para la actualización de componentes del servidor

En la siguiente tabla se enumeran las versiones de firmware admitidas para los componentes del servidor cuando el firmware de PowerEdge FX2/FX2s de la CMC se actualiza de la versión 2.0 a la 2.1, pero los componentes del servidor no se actualizan a la siguiente versión.

Tabla 5. 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)
FD332	FIRMWARE de SAS RAID	25.2.2-0004	25.4.0.0015
FC430	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
FC630	iDRAC	2.52.52.52	2.52.52.52
	Lifecycle Controller	2.52.52.52	2.52.52.52
	Diagnóstico	4239.44	4239A36
	BIOS	2.6.0	2.7.1
FC830	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnóstico	4239.44	4239A36

Tabla 5. Versiones admitidas de los componentes del servidor para la actualización de componentes del servidor a la versión N (continuación)

Plataforma	Componente del servidor	Versión anterior de cada componente (versión N-1)	Versión actualizada de cada componente (versión N)
	BIOS	2.6.0	2.7.1
FM120x4	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnóstico	4231A0	4247A1
	BIOS	1.6.0	1.7.0
FC640	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

Adaptadores de red admitidos

La siguiente tabla enumera los adaptadores de red admitidos para PowerEdge FX2/FX2s.

Tabla 6. Adaptadores de red admitidos para PowerEdge FX2/FX2s

	Plataformas			
Modelo	**FC430**	**FC630**	**FC830**	**FC640**
5718 DP 1G	Sí	Sí	No	Sí
57810S 10G SFP+	No	Sí	No	Sí
57810S 10G BASE-T	No	Sí	No	Sí
5719 QP 1G	Sí	Sí	Sí	Sí
5720 DP 1G	Sí	No	No	Sí
57416 DP 10G	No	No	No	Sí
57414 DP 25G	No	No	No	Sí
57412 DP 10G	No	No	No	Sí
BCOM QP 1G	Sí	Sí	Sí	Sí
LightPulse LPE12002 FC8 HBA	Sí	Sí	Sí	Sí
LightPulse LPe15002B-M8-D DP 8G Gen 5	Sí	Sí	Sí	Sí
HBA FC 16 de puerto dual LPe16002	Sí	Sí	Sí	Sí
LightPulse LPE12000 FC 8 HBA	No	Sí	Sí	Sí
LightPulse LPe 15000B-M8-D SP 8G Gen 5	No	Sí	Sí	Sí
HBA FC 16 de puerto único LPE 16000	No	Sí	Sí	Sí
LPE 31K0 FC16 1P	No	Sí	Sí	Sí
LPE32002 FC32 2P	No	Sí	Sí	Sí
LPE31K2 FC16 2P	Sí	Sí	Sí	Sí

Tabla 6. Adaptadores de red admitidos para PowerEdge FX2/FX2s (continuación)

	Plataformas			
Modelo	**FC430**	**FC630**	**FC830**	**FC640**
LPE 32000 FC32 1P	No	Sí	Sí	Sí
OCe 14102-UX-D CNA de 10 GbE	No	No	No	No
OCe 14102-U1-D CNA de 10 GbE	Sí	Sí	Sí	Sí
OCe 14102-U1-D CNA de 10 GbE	Sí	Sí	Sí	Sí
X540 DP 10G BASE-T	Sí	Sí	Sí	Sí
I350 DP 1G	Sí	Sí	Sí	Sí
I350 QP 1G	Sí	Sí	Sí	Sí
X520 DP 10G SFP+	No	Sí	No	Sí
X710 DP 10GBE SFP+ (Fortville)	Sí	Sí	Sí	Sí
CX3 DP 40GbE QSFP+	Sí	Sí	Sí	Sí
CX3 DP 10GbE DA/SFP+	Sí	Sí	Sí	Sí
CX3 MCX354-A-FCBT	No	No	No	No
HBA QLE2560 FC8 de un canal	No	Sí	Sí	Sí
57810S 10G BASE-T	Sí	Sí	Sí	Sí
QLE2660 SP FC 16 HBA	No	Sí	Sí	Sí
QLE2662 DP FC16 HBA	Sí	Sí	Sí	Sí
QLG SFP DP 10G	No	No	No	Sí
QLG BT DP 10G	No	No	No	Sí
QLE2560 FC 8 HBA	No	Sí	Sí	Sí
QLG SFP DP 25G	No	No	No	Sí
QLE2562 FC8 HBA	Sí	Sí	Sí	Sí
QLE2690 FC16 SP HBA	No	Sí	Sí	Sí
QLE2742 FC32 SFP+ HBA	No	Sí	Sí	Sí
QLE2740 FC32 SP HBA	No	Sí	Sí	Sí
QLE2692 FC16 DP HBA	Sí	Sí	Sí	Sí
PCIE SF852P DP 10G	Sí	Sí	Sí	Sí
INTEL OPA x16 LP	No	No	Sí	Sí

Administración de licencias

Las funciones de la CMC están disponibles según la licencia adquirida (CMC Express o CMC Enterprise). 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, etc. 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.

Licencias de sled de almacenamiento

También puede adquirir licencias de sled de almacenamiento para administrar controladoras RAID en la CMC. Las licencias de sled de almacenamiento se pueden instalar en la fábrica o comprar en línea. A continuación, se mencionan los tipos de licencia de sled de almacenamiento compatibles:

- Una controladora RAID y una controladora HBA (RAID/HBA)
- Dos controladoras RAID

Las licencias de sled de almacenamiento se pueden utilizar para una o dos controladoras RAID. Si se asigna una licencia a RAID en una sola controladora, la licencia se aplica únicamente a la primera controladora. La eliminación de una licencia de sled de almacenamiento puede provocar la pérdida de datos de RAID.

Las licencias de sled de almacenamiento son específicas de un sled de almacenamiento y están asociadas a la etiqueta de servicio del sled de almacenamiento. Por ejemplo, si transfiere un sled de almacenamiento de un chasis a otro, la licencia también se transfiere junto con el sled de almacenamiento. Las copias maestras de licencias de sled de almacenamiento se almacenan en el almacén persistente. Para obtener más información, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/manuals**.

Los mensajes de registro de todas las actividades de licencia del sled de almacenamiento se almacenan en el archivo de registro de la CMC.

NOTA: Se necesitan las licencias de sled de almacenamiento para cambiar las controladoras RAID FD33xS y FD33xD del modo HBA al modo RAID.

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 por otros 30 días. Las licencias de evaluación se basan en períodos de tiempo y el cronómetro comienza a funcionar cuando se suministra alimentación al sistema. Estas licencias no se aplican a los sleds de almacenamiento.
- Perpetua: la licencia está enlazada a la etiqueta de servicio y es permanente.

NOTA: Las licencias de evaluación y sitio solo se aplican a la CMC.

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 enlace disponible al portal de autoservicio. Haga clic en él para abrir el Portal de autoservicio de licencias en Internet desde el cual 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 realizar las tareas de administración de licencias, asegúrese de adquirir las licencias. Para obtener más información, consulte la sección Adquisición de licencias y la *Guía de información general y funciones* que está disponible en **dell.com/support**. 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: vea la información de la licencia actual para la CMC y los sled de almacenamiento.
- 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 pasa las comprobaciones de validación.

  NOTA: Para algunas funciones, su activación requiere un reinicio del sistema.

También puede importar licencias para los sled de almacenamiento que están instalados en un chasis y cuando se apagan los sled de almacenamiento. Si ya tiene licencia para un sled de almacenamiento, elimine la licencia existente antes de importar una nueva. La licencia importada se almacena en License Manager de la CMC y en el almacén persistente del sled de almacenamiento. Las funciones con licencia solo están disponibles si el RAID se restablece cuando se reinicia el servidor host. Puede importar licencias de sled de almacenamiento solo al dispositivo objetivo.

- Exportar: exporte la licencia instalada en un dispositivo de almacenamiento externo como copia de seguridad o para reinstalarla después de reemplazar la parte de servicio. El nombre de archivo y el formato de la licencia exportada es `<EntitlementID>.xml`
- Eliminar: elimine la licencia asignada a un componente o sled de almacenamiento si falta dicho componente o sled de almacenamiento. Una vez eliminada la licencia, ya no se almacenará en la CMC y se activarán las funciones del producto base.

  Puede eliminar las licencias de sled de almacenamiento solo cuando dicho sled de almacenamiento está apagado. Las licencias eliminadas se eliminan del almacén persistente del sled de almacenamiento y License Manager.

- 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.

  En el caso de los sled de almacenamiento, la nueva licencia sobrescribe la licencia existente en License Manager de la CMC y el almacén persistente del sled de almacenamiento. Apague los sled de almacenamiento antes de reemplazar la licencia. Las funciones con licencia están disponibles solo después de restablecer la controladora RAID en el siguiente reinicio del host.

- 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, consulte el Portal de administración de licencias de Dell Software disponible en **WWW.DELL.COM/SUPPORT/LICENSING/US/EN/19**
- 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.

  NOTA: Si intenta instalar la licencia de PowerEdge FM120x4 en PowerEdge FC630, se produce un error en la instalación de la licencia. Para obtener más información acerca de las licencias, consulte la *Guía de usuario de Integrated Dell Remote Access Controller (iDRAC)*.

Funciones con licencia en la CMC

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

Tabla 7. Funciones del CMC basadas en los tipos de licencia

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

Tabla 7. Funciones del CMC basadas en los tipos de licencia (continuación)

Función	Express	Enterprise
Restauración de configuración de CMC	Sí	Sí
Syslog remoto	No	Sí
Servicios de directorio	No	Sí
Asistencia de inicio de sesión único	No	Sí
Autentificación de dos factores	No	Sí
Autenticación de PK	No	Sí
Recurso compartido de archivos remotos	No	Sí
Límite del nivel de alimentación del gabinete	No	Sí
Administración de chasis múltiples	No	Sí
Activación de FlexAddress	No	Sí
Actualización de firmware del servidor de uno a muchos	No	Sí
Configuración de uno a muchos para iDRAC	No	Sí

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 8. 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

Visualización de versiones traducidas de la interfaz web de la CMC

Para ver las versiones traducidas de la interfaz web del CMC, lea la documentación del explorador web. Para ver las versiones traducidas, configure el explorador en el idioma deseado.

Aplicaciones admitidas de la consola de administración

La 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 utilizar 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 la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s* 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 los comandos RACADM, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/manuals**.

Otros documentos que puede necesitar

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

- En *CMC FX2/FX2s Online Help* (Ayuda en línea de la CMC para FX2/FX2s) se ofrece información acerca de cómo usar la interfaz web. Para acceder a la ayuda en línea, haga clic en **Ayuda** en la interfaz web del CMC.
- En la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller versión 2.0 para Dell PowerEdge FX2/FX2s* se proporciona información sobre cómo utilizar las funciones RACADM relacionadas con FX2/FX2s.
- En las *Notas de publicación de Dell Chassis Management Controller (CMC) para Dell PowerEdge FX2/FX2s versión 2.0* disponible en **dell.com/cmcmanuals** se proporcionan actualizaciones de último minuto para el sistema así como documentación o material de referencia con información técnica avanzada para técnicos o usuarios experimentados.
- En *Integrated Dell Remote Access Controller 8 (iDRAC) User's Guide* (Guía del usuario de Integrated Dell Remote Access Controller 8 [iDRAC]), se ofrece información sobre la instalación, la configuración y el mantenimiento del iDRAC8 en sistemas administrados.
- 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.
- 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 siguiente documentación del sistema proporciona más información sobre el sistema en la que está instalada la CMC PowerEdge FX2/FX2s:

- 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 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 Quick Resource Locator (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:

- En el caso de los documentos de Dell EMC Enterprise Systems Management: **www.dell.com/SoftwareSecurityManuals**
- En el caso de los documentos de Dell EMC OpenManage: **www.dell.com/OpenManageManuals**
- En el caso de los documentos de Dell EMC Remote Enterprise Systems Management: **www.dell.com/esmmanuals**
- Para ver documentos de iDRAC: **www.dell.com/idracmanuals**
- Para ver documentos de Dell EMC OpenManage Connections Enterprise Systems Management: **www.dell.com/OMConnectionsEnterpriseSystemsManagement**
- En el caso de los documentos de las herramientas de facilidad de reparación de Dell EMC: **www.dell.com/ServiceabilityTools**
- 1. Vaya a **www.support.dell.com**.
  2. Haga clic en **Examinar todos los productos**.
  3. En la página **Todos los productos**, haga clic en **Software** y luego haga clic en el vínculo requerido de lo siguiente:
     - **Análisis**
     - **Administración de sistemas cliente**
     - **Aplicaciones empresariales**
     - **Enterprise Systems Management (Administración de sistemas empresariales)**
     - **Soluciones para el sector público**
     - **Utilidades**
     - **Mainframe**
     - **Serviceability Tools (Herramientas de servicio)**
     - **Soluciones de virtualización**
     - **Sistemas operativos**
     - **Asistencia**
  4. Para ver un documento, haga clic en el producto requerido y, luego, en la versión requerida.
- Mediante los motores de búsqueda:
  - Escriba el nombre y la versión del documento en el cuadro de búsqueda.

2

Instalación y configuración de la 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.

Temas:

Instalación de hardware de la CMC

La CMC está preinstalada en el chasis, por lo que no se requiere su instalación.

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 con la etiqueta **GB1** a la red de administración.

   Red de administración: CMC y el iDRAC (en cada servidor) y los puertos de administración de red de todos los módulos de E/S del conmutador se conectan a una red interna común en el chasis PowerEdge FX2/FX2s. Esto permite aislar la red de administración de la red de datos de servidores.

   Red de aplicación: el acceso a los servidores administrados se realiza mediante conexiones de red a los módulos de E/S (IOM). Esto permite aislar la red de aplicaciones de la red de administración. Es importante separar el tráfico para garantizar el acceso ininterrumpido a las funciones de administración del chasis.

   NOTA: 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 como fuera de línea 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.
2. El puerto STK/GB2 también se puede utilizar para la conmutación por error de NIC de la CMC. Asegúrese de que el valor de configuración predeterminado de la CMC se cambia del valor predeterminado **Apilamiento** a **Redundante** para implementar la conmutación por error de NIC. Para obtener más información, consulte Configuración de puerto de administración 2.

   PRECAUCIÓN: La conexión del puerto STK/Gb2 a la red de administración producirá resultados impredecibles si la configuración de la CMC no se ha cambiado del valor predeterminado Apilamiento a Redundante para implementar la conmutación por error de NIC. En el modo de apilamiento predeterminado, el cableado de los puertos Gb1 y STK/Gb2 a la misma red (dominio de difusión) puede producir una saturación por difusión. También se puede producir una saturación por difusión si la configuración de CMC se cambia al modo redundante, pero el cableado está conectado en cadena tipo margarita entre el chasis en el modo de apilamiento. Asegúrese de que el cableado modelo coincide con la configuración de CMC para el uso previsto.
3. Instale el módulo de E/S en el chasis y conecte el cable de red al módulo de E/S.
4. Inserte los servidores en el chasis.
5. Conecte el chasis a la fuente de alimentación.

6. Para encender el chasis, presione el botón de encendido o utilice las siguientes interfaces después de completar la tarea 6. Mediante la interfaz web, vaya a **Visión general del chasis** > **Alimentación** > **Control** > **Opciones de control de alimentación** > **Encender sistema**. Haga clic en **Aplicar**.

   También puede encender el chasis mediante la interfaz de línea de comandos, utilice el comando `racadm chassisaction powerup` para llevar a cabo dicha acción.

   NOTA: No encienda los servidores.

7. La configuración de red de la CMC predeterminada es estática con la dirección IP de la CMC 192.168.0.120. Si desea cambiar la configuración de la red a DHCP, conecte un cable de serie al puerto serie de la CMC. Para obtener más información acerca de la conexión en serie, consulte la configuración de interfaz serie/protocolo de configuración en la sección Uso de software de acceso remoto desde una estación de administración.

   Una vez que se haya establecido la conexión en serie, inicie sesión y utilice el comando `racadm setniccfg –d` para cambiar la configuración de la red a DHCP. La CMC demora entre 30 y 60 segundos aproximadamente en obtener la dirección IP desde el servidor DHCP.

   Para ver la dirección IP de la CMC asignada por DHCP, utilice uno de los siguientes métodos:

   - Para ver la dirección IP de la CMC mediante una conexión serie con la CMC, lleve a cabo los siguientes pasos:
     a. Conecte un extremo del cable de módem nulo serie al conector serie en la parte posterior del chasis.
     b. Conecte el otro extremo del cable al puerto serie del sistema de administración.
     c. Una vez establecida la conexión, inicie sesión en la CMC con las credenciales de la cuenta raíz predeterminada.
     d. Ejecute el comando `racadm getniccfg`.

        En la salida que se muestra, busque **Dirección IP actual**.

   - Para ver la dirección IP de la CMC conectándose al servidor mediante KVM, lleve a cabo los siguientes pasos:
     a. Conéctese a un servidor en el chasis mediante KVM.
        NOTA: Para obtener más detalles acerca de cómo conectar con un servidor mediante KVM, consulte Cómo acceder al servidor mediante KVM.
     b. Encienda el servidor.
     c. Asegúrese de que el servidor está configurado para el inicio en Unified Extensible Firmware Interface (UEFI).
     d. Presione F2 para abrir la página Configuración del sistema.
     e. En la página **Configuración del sistema**, haga clic en **Configuración del iDRAC** > **Resumen del sistema**.

        La dirección IP de la CMC se muestra en la sección **Chassis Management Controller**.

        Para obtener más información acerca de la página **Configuración del iDRAC** en la interfaz gráfica de usuario del iDRAC, consulte la *Guía del usuario de Dell Integrated Dell Remote Access Controller (iDRAC)*.

8. Conecte a la dirección IP del CMC mediante un explorador web al escribir la credencial de la cuenta raíz predeterminada.
9. Configure los valores de red del iDRAC según sea necesario. De forma predeterminada, la LAN de iDRAC está activada con la IP estática configurada. Para determinar la dirección IP estática predeterminada con una **licencia de Enterprise**, vaya a **Descripción general del servidor** > **Configuración** > **iDRAC**. También puede determinar la dirección IP estática con una **licencia Express**. Vaya a **Visión general del servidor** > **Servidor-ranura** > **Configuración** > **iDRAC**.
10. Proporcione el módulo de E/S con una dirección IP de administración externa (si corresponde) 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**.
11. Establezca conexión con cada iDRAC a través de la interfaz web mediante la credencial de la cuenta raíz predeterminada a fin de completar cualquier configuración necesaria.
12. Encienda los servidores e instale el sistema operativo.

NOTA: La credencial de cuenta local predeterminada es root (nombre de usuario) y calvin (contraseña de usuario).

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

Conexión en cadena tipo margarita de la CMC a la red de FX2

Si tiene varios chasis en un bastidor, puede reducir la cantidad de conexiones a la red de administración mediante una conexión en cadena margarita de hasta diez chasis. Puede reducir la cantidad de conexiones ascendentes requeridas de la red de administración de diez a una.

Cuando se conectan los chasis mediante una cadena margarita, GB es el puerto de enlace ascendente y STK es el puerto de apilamiento (consolidación de cables). Conecte los puertos Gb a la red de administración o al puerto STK de la CMC en un chasis que esté más cerca de la red. Conecte el puerto STK únicamente a un puerto Gb que esté lo más alejado posible de la cadena o red.

En la ilustración siguiente se muestra la organización de cables de cuatro chasis conectados en cadena tipo margarita, todos con CMC activas.

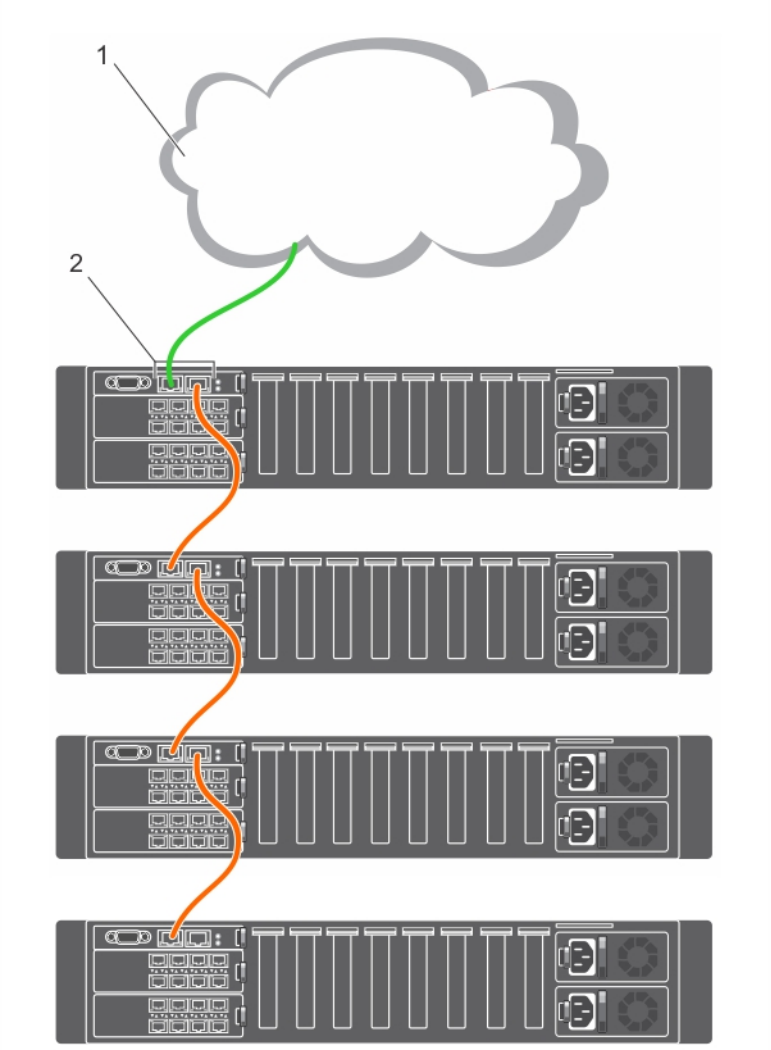
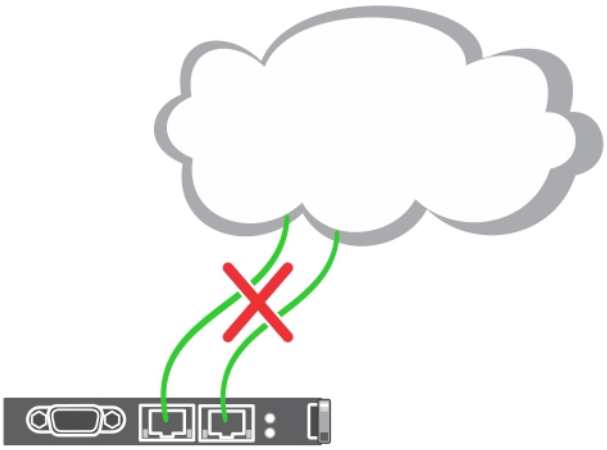


Tabla 9. Conexión en cadena tipo margarita de sleds de almacenamiento

Número de componente en la imagen	Nombre del componente
1	Red de administración
2	CMC activa

La siguiente figura muestra un ejemplo de cableado incorrecto de la CMC en modo de apilamiento



A continuación se detallan los pasos para la conexión en cadena tipo margarita de cuatro módulos de la CMC de FX2:

1. Conecte el puerto GB de la CMC de FX2 del primer chasis a la red de administración.
2. Conecte el puerto GB de la CMC de FX2 del segundo chasis al puerto STK de la CMC de FX2 del primer chasis.
3. Si existe un tercer chasis, conecte el puerto GB de la CMC de FX2 al puerto STK de la CMC de FX2 del segundo chasis.
4. Si existe un cuarto chasis, conecte el puerto GB de la CMC de FX2 al puerto STK de la CMC de FX2 del segundo chasis.

PRECAUCIÓN: Nunca debe conectar el puerto STK de alguna CMC a la red de administración. Solo se puede conectar al puerto GB de otro chasis. Conectar un puerto STK a la red de administración puede interrumpir la red y provocar una pérdida de datos. Conectar GB y STK por cable a la misma red (dominio de difusión) puede provocar una tormenta de difusión.

NOTA: Restablecer un CMC cuyo puerto STK está conectado en cadena a otra CMC puede interrumpir la red para las CMC que aparezcan más adelante en la cadena. Las CMC secundarias pueden registrar mensajes que indican que se perdió el enlace de red.

NOTA: Cuando se conectan los chasis mediante una cadena margarita, asegúrese de que todos los chasis compartan el mismo ID de VLAN.

Uso del software de acceso remoto desde una estación de administración

Puede acceder a la CMC desde una estación de administración mediante varios softwares de acceso remoto. A continuación, se proporciona una lista de softwares de acceso remoto de Dell disponibles en su sistema operativo.

Tabla 10. Interfaces del CMC

Interfaz/ protocolo	Descripción
Serie	La CMC admite una consola de texto de serie que se puede iniciar mediante cualquier software de emulación de terminal. A continuación, se incluyen algunos ejemplos de este tipo de software que se puede utilizar para conectarse a la CMC. • Minicom de Linux • HyperTerminal de Hilgraeve para Windows Conecte un extremo del cable de módem nulo serie (presente en ambos extremos) al conector serie en la parte posterior del chasis. Conecte el otro extremo del cable al puerto de serie de la estación de administración. Para obtener más información sobre la conexión de cables, consulte el panel posterior del chasis en la sección Descripción general del chasis. Configure su software de emulación de terminal con los siguientes parámetros:

Tabla 10. Interfaces del CMC (continuación)

Interfaz/ protocolo	Descripción
	• Velocidad en baudios: 115200 • Puerto: COM1 • Datos: 8 bits • Paridad: ninguna • Detener: 1 bit • Control de flujo de hardware: Sí • Control de flujo de softwarel: No
Remote RACADM CLI	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 de RACADM en una red, requiere la IP de la CMC, el nombre de usuario y la contraseña Para utilizar el RACADM remoto desde la estación de administración, instale el RACADM remoto con el uso del DVD Documentación y herramientas de Dell Systems Management que está disponible con el sistema. Para obtener más información sobre el RACADM remoto.
Web Interface	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 **Exploradores admitidos** en la matriz de soporte del software de Dell System en **dell.com/support/manuals**.
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 conectarse 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.
SNMP	El Protocolo simple de administración de redes (SNMP) es un conjunto de definiciones de protocolo para administrar dispositivos en la red. La CMC proporciona acceso a SNMP, lo cual le permite utilizar las herramientas SNMP para hacer una consulta en la CMC y obtener información de administración de sistemas. El archivo MIB de la CMC se puede descargar desde la interfaz web de la CMC, vaya a **Descripción general del chasis** > **Red** > **Servicios** > **SNMP**. Consulte la *Guía de referencia de SNMP de Dell OpenManage* para obtener más información acerca del MIB de la CMC. En el siguiente ejemplo se muestra cómo se puede utilizar el comando `net-snmp snmpget` para obtener la etiqueta de servicio del chasis de la CMC. `snmpget -v 1 -c <CMC community name> <CMC IP address>.1.3.6.1.4.1.674.10892.2.1.1.6.0`
WSMan	Los servicios WSMan se basan en el protocolo Web Services for Management (WSMan) para realizar tareas de administración de uno a varios sistemas. Puede utilizar el cliente WSMan como cliente WinRM (Windows) o el cliente OpenWSMan (Linux) para utilizar la funcionalidad 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. **NOTA:** El puerto SSL que se utiliza para la seguridad de transporte es el mismo que el puerto HTTPS de la CMC.

Tabla 10. Interfaces del CMC (continuación)

Interfaz/ protocolo	Descripción
	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 WS-Management: **www.dmtf.org/standards/wbem/wsman** 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**>.

Inicio de la CMC mediante otras herramientas de Systems Management

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

Para acceder 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** > **Controladora de acceso remoto**. Para obtener más información, consulte la *Guía del usuario de Dell Server Administrator* en **dell.com/support/manuals**.

Instalación de RACADM remoto

Para utilizar el RACADM remoto desde la estación de administración, instale el RACADM remoto con el uso del DVD *Documentación y herramientas de Dell Systems Management*. 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 información sobre la instalación de los componentes de Dell OpenManage Software Dell, consulte la *Guía del usuario de instalación y seguridad de Dell OpenManage* disponible en **dell.com/support/manuals**. También puede descargar la versión más reciente de las herramientas de DRAC de Dell desde **support.dell.com**.

Instalación de RACADM remoto en una estación de administración con Windows

Si está utilizando el DVD, ejecute ***<path>*\SYSMGMT\ManagementStation\windows\DRAC*<.msi file name>***

Si ha descargado el software desde **dell.com/support**:

1. Extraiga el archivo descargado y ejecute el archivo **.msi** que se proporciona.
   Dependiendo de la versión descargada, el archivo se denominará DRAC.msi, RACTools.msi, o RACTools64Bit.msi.
2. Acepte el contrato de licencia Haga clic en **Siguiente**.
3. Seleccione la ubicación donde se instalará. **Haga clic en Siguiente**.
4. Haga clic en **Instalar**.
   Aparecerá la ventana de instalación.

5. Haga clic en **Finalizar**.

Abra un símbolo del sistema del comando administrador, escriba `racadm` y presione **Intro**. Si aparecen las instrucciones de ayuda de RACADM, significa que el software está instalado correctamente.

Instalación de RACADM remoto 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 *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 permite iniciar ningún archivo ejecutable desde el DVD. Debe montar el DVD-ROM manualmente y, a continuación, ejecutar los comandos.

4. Vaya al directorio **SYSMGMT/ManagementStation/linux/rac**. Para instalar el software de 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 la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge FX2/FX2s*.

   NOTA: Cuando se utiliza la funcionalidad 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 remoto desde una estación de administración con Linux

1. Inicie sesión como `root` en el sistema en el que desea desinstalar las funciones de la estación de administración.
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 rpm `-e rpm -qa | grep mgmtst-racadm`.

Configuración de un explorador web

Puede configurar y administrar la CMC, los servidores y los módulos instalados en el chasis a través de un navegador web. Consulte la sección "Navegadores compatibles" en la correspondiente en *Matriz de compatibilidad de software de los sistemas Dell* en **dell.com/support/manuals**.

La CMC y la estación de administración, donde utiliza el navegador, deben estar en la misma red, la cual se denomina *red de administración.* Según sus 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, algunos ajustes 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 un servidor proxy que no posee acceso a la red de administración, puede agregar las direcciones de la red de administración a la lista de excepciones del explorador. Esto indica al explorador que pase por alto el servidor proxy cuando intente obtener acceso a la red de administración.

Filtro de suplantación de identidad de Microsoft

Si se activa el filtro de suplantación de identidad de Microsoft en el sistema de administración 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**.

Descarga de archivos desde la 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, un ícono de transferencia de archivos gira para mostrar la actividad de transferencia. Si se utiliza Internet Explorer, se 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**.

Descarga y actualización de firmware de la CMC

Para descargar el firmware del CMC, consulte Descarga de firmware del CMC.

Para actualizar el firmware del CMC, consulte 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 **cmc-“Etiqueta de servicio”**). 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**, escriba las propiedades de ubicación y el nombre del chasis. Para obtener más información sobre cómo establecer las propiedades del chasis, consulte la *Ayuda en línea para CMC*.

   Puede ver el nombre del chasis cuando inicia sesión en CMC mediante SSH; para ello, seleccione **Mostrar nombre del chasis en indicador SSH**. De manera predeterminada, se desmarca la opción **Mostrar nombre del chasis en indicador SSH**.

   NOTA: El campo **Ubicación del chasis** es opcional. Utilice 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**.

Por ejemplo, `racadm setsysinfo –c chassisname` o `racadm setsysinfo –c chassislocation`

Para obtener más información, consulte la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2/FX2s*.

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

Para establecer la fecha y la hora con la inferfaz de línea de comandos, consulte el comando **config** y las secciones de los grupos de bases de datos de propiedad `cfgRemoteHosts` en la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/manuals**.

Por ejemplo, `racadm setractime -l 20140207111030`.

Para leer la fecha y la hora, utilice el comando `racadm getractime`.

Configuración de los LED para identificar componentes en el chasis

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

NOTA: Para modificar esta configuración, debe tener privilegios de **Administrador de comandos de depuración** en una CMC.

Cuando un sled de cálculo realiza una acción de identificación, el LED frontal del sled de almacenamiento conectado también hace parpadear al patrón de identificación. Si un sled de almacenamiento está en modo único dividido y está conectado a dos nodos de cálculo, deberá hacer parpadear el patrón de identificación si alguno de los dos nodos de cálculo está realizando una acción de identificación.

Si inicia una acción de identificar mediante OMSS o iDRAC para un sled de cálculo, una unidad o un gabinete, el sled de almacenamiento asociado con ellos también realiza la acción de identificar.

NOTA: No puede seleccionar solo sleds de almacenamiento para una acción de identificar.

Configuración del parpadeo de LED mediante la interfaz web de la 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.

Para activar el parpadeo del LED de un componente, seleccione el componente correspondiente y haga clic en **Parpadear**. Para desactivar el parpadeo del LED de un componente, deseleccione el servidor y haga clic en **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 (PowerEdge FM120x4), y `server-nx` donde *n* = 1–4 y *x* = de a a b (PowerEdge FC630).
- `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

Configuración de las propiedades de la 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 panel frontal

Puede utilizar la página del panel frontal para configurar:

- Botón de encendido
- KVM

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.

Acceso a un servidor mediante KVM

Para asignar un servidor a KVM desde la interfaz web:

1. Conecte un monitor al conector de video y un teclado al conector USB ubicado en la parte frontal del chasis.
2. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Panel anterior** > **Configuración**.

3. En la página **Configuración del panel anterior**, en la sección **Configuración de KVM**, seleccione la opción **Activar asignación de KVM**.
4. En la página **Configuración del panel anterior**, en la sección **Configuración de KVM**, para la opción **KVM asignado**, seleccione el servidor que desee de la lista desplegable.
5. Haga clic en **Aplicar**.

Para asignar un servidor a KVM mediante racadm, utilice el comando `racadm config -g cfgKVMInfo -o cfgKvmMapping [server slot #]`.

Para ver la asignación actual de KVM mediante racadm, utilice `racadm getconfig -g cfgKVMInfo`.

Configuración de la administración del chasis en modo de servidor

Esta función le permite administrar y supervisar los componentes compartidos del chasis y los nodos del chasis como servidores de bastidor. Cuando esta función está activada, puede usar el proxy RACADM del iDRAC, los sistemas operativos de servidores blade y Lifecycle Controller para realizar lo siguiente:

- Supervisar y administrar ventiladores del chasis, fuentes de alimentación y sensores de temperatura
- Actualizar y configurar el firmware de la CMC

Configuración de la administración del chasis en el servidor mediante la interfaz web de la CMC

Para activar la administración del chasis en modo servidor:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Configuración** > **General**.
2. En la página **Configuración general del chasis**, en el menú desplegable **Administración del chasis en modo servidor**, seleccione uno de los siguientes modos:
   - **Ninguno**: este modo no le permite supervisar ni administrar el componente del chasis a través del iDRAC, el sistema operativo o Lifecycle Controller.
   - **Supervisar**: este modo le permite supervisar los componentes del chasis pero no puede realizar ninguna actualización de firmware a través del iDRAC, el sistema operativo, el proxy de RACADM del iDRAC o Lifecycle Controller.
   - **Administrar y supervisar**: este modo le permite supervisar los componentes del chasis y actualizar el firmware de la CMC mediante DUP a través del iDRAC, el sistema operativo, RACADM del iDRAC o Lifecycle Controller.

Configuración de la administración del chasis en modo de servidor mediante RACADM

Para activar la administración del chasis en el servidor mediante RACADM, utilice los siguientes comandos:

- Para desactivar la administración del chasis en modo de servidor, utilice:

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 0
```

- Para cambiar la administración del chasis en modo de servidor a supervisar, utilice:

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 1
```

- Paa cambiar la administración del chasis en modo de servidor a administrar y supervisar, utilice:

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 2
```

3

Inicio de sesión en la 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. También puede iniciar sesión mediante un inicio de sesión único o una tarjeta inteligente.

Temas:

Configuración de la autentificación de clave pública en SSH

Puede configurar hasta seis claves públicas que pueden utilizarse con el nombre de usuario del servicio en una interfaz de SSH. Antes de agregar o eliminar claves públicas, asegúrese de usar el comando `view` para ver las claves que ya están configuradas, de modo que una clave no se sobrescriba ni se elimine accidentalmente. El nombre de usuario del servicio es una cuenta de usuario especial que se puede utilizar cuando se accede a la CMC a través de SSH. Cuando se configura y se utiliza correctamente la PKA en SSH, no es necesario ingresar un nombre de usuario ni una contraseña para iniciar sesión en la CMC. Esto puede ser muy útil para configurar scripts automatizados con el fin de ejecutar diversas funciones.

NOTA: No hay soporte de interfaz gráfica de usuario para administrar esta función; solamente se puede utilizar RACADM.

Cuando se agregan claves públicas nuevas, asegúrese de que las claves existentes no se encuentren en el índice, donde se agrega la clave nueva. La CMC no realiza comprobaciones para asegurarse de que las claves anteriores se eliminen antes de agregar una nueva. Ni bien se agrega una clave nueva, esta entra en vigor automáticamente, siempre y cuando la interfaz de SSH esté activada.

Cuando utilice la sección comentario de clave pública de la clave pública, recuerde que la CMC utiliza solo los primeros 16 caracteres. La CMC utiliza el comentario de clave pública para distinguir a los usuarios SSH cuando usan el comando RACADM `getssninfo`, ya que todos los usuarios de PKA utilizan el nombre de usuario del 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 la *Guía de referencia de la línea de comandos de Chassis Management Controller para PowerEdge FX2/FX2s*.

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 mediante 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 en 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 para el tipo de clave que generará (SSH-1 no es compatible).
2. Ingrese la cantidad de bits para la clave. Asegúrese de que el tamaño de la clave de RSA sea entre 1024 y 4096.

   NOTA:
   - Es posible que la CMC no muestre un mensaje si se agregan claves menores a 1024 o mayores a 4096, pero estas claves fallan al intentar iniciar sesión.
   - La CMC acepta las claves RSA hasta la clave 4096, pero la fortaleza recomendada de la clave es 1024.

3. Haga clic en **Generar** y mueva el mouse en la ventana 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, en el indicador de shell, escriba:

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

donde:

`-t` debe ser 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.

El *passphrase* es opcional. Después de completar el comando, utilice el archivo público para pasar a RACADM y cargar el archivo.

Acceso a la interfaz web de la CMC

Antes de iniciar sesión en la CMC mediante la interfaz web, asegúrese de haber configurado un explorador web compatible 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 mediante la dirección IPv4: `https://<CMC IP address>`

     Si el número de puerto HTTPS predeterminado (puerto 443) se ha cambiado, escriba: `https://<CMC IP address>:<port number>`
   - Para acceder a la CMC mediante 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 la CMC como usuario local, usuario de Active Directory o usuario LDAP

Para iniciar sesión en la CMC, debe tener una cuenta de CMC con el privilegio **Iniciar sesión en la CMC**. La cuenta raíz predeterminada es la cuenta de administración predeterminada que se envía con la CMC.

NOTA: Para una mayor seguridad, se recomienda cambiar la contraseña predeterminada de la cuenta raíz durante la configuración inicial.

NOTA: Cuando la validación de certificados está activada, se 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 fallará.

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>

     NOTA: El nombre de usuario de la CMC solo puede contener caracteres alfanuméricos y determinados caracteres especiales. No se admiten el símbolo de arroba (@) ni los siguientes caracteres especiales:

     - Diagonal (/)
     - Barra de retroceso (/)
     - Punto y coma (;)
     - Cita de retroceso (')
     - Doble comilla (")
   - 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 campo **Dominio**, en el menú desplegable, 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 la sesión se cierre automáticamente. El valor predeterminado es el **Límite de tiempo de inactividad 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 lal CMC mediante una tarjeta inteligente

Para usar esta función, debe tener una licencia Enterprise. Es posible iniciar sesión en la CMC mediante una tarjeta inteligente. Las tarjetas inteligentes proporcionan una Autenticación de dos factores (TFA), lo cual representa 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), acceda a 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 la CMC mediante 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 autentificación 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 iniciar sesión en el SSO. 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 conecta utilizando las credenciales de Kerberos que el explorador almacenó en caché cuando inició sesión utilizando su cuenta de Active Directory válida. Si no se pudo iniciar sesión, el explorador vuelve 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.

Inicio de sesión en la CMC mediante una consola serie, Telnet o SSH

Es posible iniciar sesión en la 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, realice las tareas siguientes para iniciar sesión en la 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.

Inicio de sesión en la 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 service, si se configuró una frase de contraseña durante la creación del par de claves pública-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 se ejecuta en segundo plano y hace transparente la introducción de la frase de contraseña. 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.

Cómo forzar un cambio de contraseña mediante la interfaz web

Puede cambiar la contraseña predeterminada cuando acceda a la interfaz de CMC por primera vez. La función se aplica en entornos accesibles a través de la red y requiere la autenticación de nombre de usuario y contraseña. Puede configurar y restablecer la función de **cambio forzado de contraseña** en cualquier momento. Es obligatorio cambiar la contraseña para iniciar sesión y acceder a la interfaz web de CMC. De forma predeterminada, el nombre de usuario es “root”.

1. Ingrese la **nueva contraseña**.
   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, ~ y \
2. Ingrese de nuevo la contraseña nueva en el cuadro de texto **Contraseña nueva**.
3. Haga clic en **Continuar** para enviar la nueva contraseña para iniciar sesión en la interfaz web de CMC.

Varias sesiones en la 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
WSMan	4

4

Actualización del firmware

Es posible actualizar el firmware para:

- La CMC
- Infraestructura del chasis
- Módulo de E/S

Es posible actualizar el firmware para los siguientes componentes del servidor:

- BIOS
- iDRAC7
- iDRAC8
- Lifecycle Controller
- Diagnósticos de 32 bits
- Paquete de controladores del sistema operativo
- Controladoras de interfaz de red
- Controladoras RAID

Temas:

Imagen de firmware de la CMC firmado

El firmware de la CMC incluye una firma. El firmware de la CMC realiza un paso de verificación 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. La actualización del firmware incluye actualización de versión o degradación.

Descarga de firmware de la 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.

Se recomienda seguir el siguiente orden de actualización al actualizar el firmware del chasis:

- El firmware de los componentes de blade
- Firmware de la CMC
- Firmware de infraestructura del chasis

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 de la 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.**

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

Puede ver las versiones de firmware actualmente instaladas mediante el comando `racadm getversion`. Para obtener más información sobre los comandos RACADM, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

Actualización de firmware de la 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.

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

NOTA: No puede actualizar el firmware de la CMC si el archivo de imagen de firmware no contiene una firma de verificación o si contiene una verificación de firma no es válida o dañada.

NOTA: No puede degradar el firmware de la CMC a una versión anterior si el firmware actual de la CMC actual no reconoce la firma calculada de la versión anterior.

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 del 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%.

Para evitar la desconexión de otros usuarios durante un restablecimiento, notifique a los usuarios autorizados que inicien 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**.

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. Luego, la CMC genera la condición general del chasis como en buen estado y se activa el enlace de red de la CMC. Una vez se haya restablecido, aparecerá la nueva versión del firmware en la página **Actualización del firmware**.

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 obtener más información sobre cómo permitir animaciones en el explorador, consulte Permitir animaciones en Internet Explorer.

NOTA: En un chasis compatible con PSU con CA de 2400 W, aparecerá un mensaje de error si intenta actualizar el firmware o cambiarlo a una versión anterior con una versión que dicha PSU no admita. Las unidades de fuente de alimentación de CA de 2400W admiten imágenes de la CMC 1.40-A00 y posteriores.

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.

Actualización de firmware de la CMC mediante la interfaz web

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 de la CMC**, seleccione los componentes requeridos en la columna **Actualizar destinos** para la CMC que desea actualizar y haga clic en **Aplicar actualización de la CMC**.
3. En el campo **Imagen del firmware**, escriba la ruta de acceso a la imagen del firmware en la estación de administración o la red compartida, o bien, haga clic en **Examinar** para buscar la ubicación del archivo. El nombre predeterminado del archivo de la imagen del firmware de la CMC es `fx2_cmc.bin`.
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. 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. Para obtener más información sobre los distintos estados del firmware, consulte la Online Help.
5. En el caso de la CMC, 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 no está conectada a la red. Debe iniciar sesión pasados unos minutos, cuando la CMC se haya reiniciado. Una vez se haya restablecido, aparecerá la nueva versión del firmware en la página **Actualización del firmware**.

   NOTA: Después de la actualización del firmware, elimine los archivos de la caché del explorador web. Para obtener instrucciones acerca de cómo borrar la 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 tarde varios minutos.

Actualización de firmware de la CMC mediante RACADM

Para actualizar el firmware de la CMC mediante RACADM, utilice el subcomando `fwupdate`.

Por ejemplo: `racadm fwupdate <options> <firmware image>`.

Para obtener más información sobre los comandos de RACADM, consulte la *Guía de referencia sobre líneas de comando de RACADM de Chassis Management Controller para PowerEdge FX2/FX2s*.

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

Actualización del firmware de la CMC mediante DUP

Puede actualizar el firmware de la CMC mediante Dell Update Package (DUP) a través de los siguientes componentes:

- Proxy de RACADM del iDRAC
- Sistema operativo del servidor blade
- Lifecycle Controller

Para obtener más información sobre la actualización del CMC a través del iDRAC, consulte la *Guía del usuario de Integrated Dell Remote Access Controller*.

Antes de actualizar la CMC mediante DUP, asegúrese de cumplir con los siguientes requisitos:

- El paquete de firmware de la CMC está disponible como DUP en un sistema local o en un recurso compartido de red.
- **Administración de chasis en modo de servidor** está establecida en **Administrar y supervisar**.

Para obtener más información, consulte Configuración de la administración del chasis en modo de servidor

- Para las actualizaciones a través del SO o Lifecycle Controller, se debe activar la opción de iDRAC **Activar la actualización de componentes compartidos a través del SO/USC**. Para obtener más información sobre cómo activar esta opción, consulte la *Guía del usuario de la Integrated Dell Remote Access Controller*.

NOTA: Cuando actualiza la CMC mediante DUP, las actualizaciones del coprocesador del módulo de E/S disponibles en la imagen de la CMC se aplican en el siguiente ciclo de encendido del chasis.

Actualización del firmware de infraestructura del chasis

La operación de actualización de la infraestructura del chasis actualiza el componente de la placa principal.

NOTA: Antes de actualizar el firmware de la infraestructura del chasis, apague todos los servidores en el chasis, en caso de ser necesario.

Actualización del firmware de infraestructura del chasis mediante la interfaz web de la 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 perderá la conexión con la CMC mientras se restablece todo el chasis. Actualice la interfaz web para iniciar sesión nuevamente. Vaya a **Descripción general del chasis** > **Controladora del chasis**.

Una vez se finalice la actualización, se mostrará la versión actualizada del firmware de la placa principal.

.

Actualización del firmware de la infraestructura del chasis mediante RACADM

Para actualizar el firmware de la infraestructura del chasis, utilice el subcomando `fwupdate`.

Por ejemplo: `racadm fwupdate <options> <firmware image>`.

Para obtener más información sobre cómo usar los comandos RACADM, consulte la *Guía de referencia de líneas de comando RACADM de Chassis Management Controller para PowerEdge FX2/FX2s*.

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

Actualización de firmware del iDRAC del servidor

Es posible actualizar el firmware para el iDRAC7 o el iDRAC8. Para usar esta función:

- Debe tener con una licencia Enterprise.
- La versión del firmware de iDRAC7 debe ser 1.57.57 o posterior.
- La versión del firmware de iDRAC8 debe ser 2.05.05 o posterior.

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

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**
   - **Visión general del chasis** > **Controladora del chasis** > **Actualizar**.

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

   NOTA:

   También puede actualizar el firmware de iDRAC del servidor mediante **Visión general del chasis** > **Visión general del servidor** > **Actualizar**. Para obtener más información, consulte Actualización del firmware de los componentes del servidor.
2. Para actualizar el firmware de iDRAC7 o iDRAC8, en la sección **Firmware Enterprise de iDRAC<número de revisión>** , haga clic en el vínculo **Actualizar** del servidor cuyo firmware desea actualizar.
   Aparecerá la página **Actualización de los componentes del servidor**. Para continuar, consulte Actualización de firmware de los componentes del servidor.

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. El firmware del iDRAC debe ser versión 2.3 o posterior para actualizar el firmware con Lifecycle Controller.

Se utilizan paquetes de actualización de Dell (DUP) para realizar las actualizaciones del firmware mediante Lifecycle Controller. El DUP de componente del paquete del controlador del sistema operativo supera este límite y se debe actualizar por separado mediante la función Almacenamiento extendido.

NOTA: Antes de utilizar la función de actualización basada en Lifecycle Controller, se deben actualizar las versiones de firmware del servidor. También 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 12.ª generación y posteriores: después de reiniciar el servidor, en los valores de F2, seleccione**Configuración de la 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:

  - iDRAC
  - Lifecycle Controller
  - BIOS

El método de actualización general de blades con un solo clic o **Actualizar desde recurso compartido de red** permite actualizar el firmware de un componente de 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 cómo utilizar el DRM para buscar las actualizaciones de firmware más recientes, consulte http://en.community.dell.com/TECHCENTER/EXTRAS/M/WHITE_PAPERS/20438118/DOWNLOAD 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 de 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 *Guía del usuario de Dell Repository Manager Data Center versión 1.8* y la *Guía del usuario de Dell Repository Manager Business Client versión 1.8* disponible en **dell.com/support/manuals**.

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, puede actualizar el firmware de los componentes del servidor en la página **Visión general del chasis** > **Visión 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.

El firmware de Lifecycle Controller se instala mediante un paquete de instalación correspondiente 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 *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.
```

NOTA: Es posible que el método "InstallFromURI" no funcione si el URI contiene espacios en blanco.

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
- BIOS
- Diagnósticos (opcional)
- Driver Pack del sistema operativo (opcional)
- RAID
- NIC
- CPLD
- 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 más información sobre Lifecycle Controller, 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 los servicios remotos de la Dell Lifecycle Controller)* o **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: privilegios de iDRAC configurados e inicio de sesión a 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 ningún tipo de operación de Lifecycle Controller en el servidor.

Elección de tipo de actualización de firmware para los componentes del servidor mediante la interfaz web de la 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** que le permite filtrar la información en función del componente está disponible solo para el modo de **Actualización por 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 el 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 que se toman después de 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 de un número de modelos de servidores y se selecciona un servidor para la actualización del BIOS, la lógica del filtro automático quita automáticamente los demás 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, una imagen de actualización del firmware del BIOS puede ser compatible con varios modelos de servidor. Estas optimizaciones se omiten si esta compatibilidad ya no se aplica en el futuro.

- El filtro automático es importante para las actualizaciones de firmware de las 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.

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 de la 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**, consulte los detalles del inventario de firmware en la sección **Inventario de firmware de componentes y dispositivos**. En esta página, puede ver la siguiente información:
   - 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 el iDRAC esté completamente operativo y luego, actualice la página para recuperar el inventario de firmware nuevamente.
   - 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 inventario de componentes y dispositivos no refleja los elementos instalados físicamente en el servidor, debe invocar el Lifecycle Controller cuando el servidor se encuentre en el proceso de inicio. Esto ayuda a actualizar la información de componentes y dispositivos internos, y le permite verificar los componentes y dispositivos instalados actualmente. Esto sucede 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 para la utilidad de configuración del iDRAC, dispone de una opción a la que se puede acceder a través de la consola de inicio:

  a. En la consola de inicio, para acceder a **Configuración del sistema**, presione <F2>.
  b. 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 dispone de opciones para realizar 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 dispositivos no admitidos pueden formar 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 consecutivas para las 4 ranuras disponibles en el chasis: ● 1, 1a, 1b, 1c, 1d ● 2, 2a, 2b, 2c, 2d ● 3, 3a, 3b, 3c, 3d ● 4, 4a, 4b, 4c, 4d Este esquema de numeración le ayuda 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, al pasar el mouse se puede 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 de trabajo se actualiza continuamente de forma dinámica. Si se detecta la finalización de un trabajo con 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. Esta información se puede consultar haciendo clic en el ícono o colocando el cursor sobre el mismo.
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 la *Guía de referencia de la línea de comandos de RACADM Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/manuals**.

Cómo guardar el informe de inventario del chasis mediante la interfaz web de la 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. Posteriormente, este repositorio se puede exportar 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 de la CMC

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

1. En la interfaz web de la 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**.
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 nuevo nombre 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 la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.
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 desmonta y vuelve a montarse 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 dispositivos no admitidos pueden formar 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: configure los privilegios para iDRAC e inicie sesión.

La operación de Lifecycle Controller programada en un servidor puede tardar entre 10 y 15 minutos en completarse. El proceso implica varios reinicios del servidor durante los cuales se instala el firmware, que también contiene una fase de verificación del firmware. Podrá ver el progreso de este proceso utilizando 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 así la cantidad de reinicios necesarios.

En ocasiones, cuando una operación se encuentra 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 indica la situación y se informa que la operación no debe enviarse. Espere a que la operación en proceso se complete y vuelva a enviarla.

No navegue fuera de la página una vez que haya enviado una operación para su programación. Si lo intenta, aparecerá un mensaje de confirmación que permite que se pueda cancelar la navegación pretendida. De lo contrario, la operación se interrumpirá. Una interrupción, principalmente durante una operación de actualización, puede finalizar la carga del archivo de imagen del firmware de manera prematura. 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 actualmente instalado para 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**, haga clic en el tipo adecuado en la sección **Seleccionar tipo de actualización**.
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

Puede instalar la imagen de firmware 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 de la CMC.

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

1. En el panel izquierdo, haga clic en **Visión general del servidor → Actualizar**.
2. En la página **Actualización de componentes del servidor**, haga clic en el tipo adecuado en la sección **Seleccionar tipo de actualización**.
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 opciones siguientes:
   - **Reiniciar ahora**: reinicia el servidor inmediatamente.
   - **En el próximo reinicio**: se reinicia manualmente el servidor en otro momento.
5. Haga clic en **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

Puede 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 actualizar el firmware de los componentes del servidor. En la página **Trabajos de Lifecycle Controller**, está disponible una lista de todos los trabajos en los servidores. 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 85MB.

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 intentan varias actualizaciones de componentes en un servidor, el tamaño combinado de todos los archivos de actualización de firmware puede superar los 85 MB. En dicho caso, una de las actualizaciones de componentes falla 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 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, algunas veces, los servicios del sistema pueden retrasar esta ejecución. En estas situaciones, la actualización falla como consecuencia de que ya no se dispone del recurso compartido remoto alojado por la CMC.

Actualización de firmware de los componentes del servidor desde un archivo mediante la interfaz web de la 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 **Visión general del servidor** y, a continuación, haga clic en **Actualizar** > **Actualización de 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 de tipo de actualización de firmware para los componentes del servidor.
3. En la sección **Filtro para actualizar componentes y dispositivos**, filtre el componente o el dispositivo (opcional). Para obtener más información, consulte CMC_Stmp_Filtrado de componentes para actualizaciones de firmware
4. En la columna **Actualizar**, seleccione las casillas de verificación para el componente o el dispositivo para el cual desea actualizar el firmware a la siguiente versión. Use el acceso directo de la tecla CRTL a fin de seleccionar un tipo de componente o dispositivo para actualizarlo en todos los servidores aplicables. Si mantiene presionada la tecla CTRL, todos los componentes se resaltarán en amarillo. Mientras mantiene presionada la tecla CRTL, seleccione el componente o el dispositivo deseado; para ello, active la casilla de verificación asociada en la columna **Actualizar**.

Se muestra una segunda tabla en la que se enumera el tipo seleccionado de componente o dispositivo y un selector para el archivo de imagen del firmware. Para cada tipo de componente, se muestra un selector para el archivo de imagen del firmware.

Algunos dispositivos como, por ejemplo, las controladoras de interfaz de red (NIC) y las controladoras RAID, contienen muchos tipos y modelos. La lógica de selección de actualizaciones filtra de manera automática el tipo de dispositivo o modelo adecuado según los dispositivos seleccionados inicialmente. El motivo principal de este comportamiento de filtrado automático es que se puede especificar solo un archivo de imagen de firmware para la categoría.

NOTA: La limitación del tamaño de actualización de un DUP único o los DUP combinados se puede ignorar si la función Almacenamiento extendido está instalada y activada. Para obtener información sobre cómo activar la función 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 los dispositivos seleccionados. Se trata de un archivo de Dell Update Package (DUP) de Microsoft Windows.
6. Seleccione una de las opciones siguientes:
   - **Reiniciar ahora**: se realiza un reinicio de inmediato. y se aplica la actualización de firmware inmediatamente.
   - **En el próximo reinicio**: se reinicia manualmente el servidor más adelante. 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 **Actualizar**. Se actualiza la versión de firmware para el componente o el dispositivo seleccionado.

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

La actualización de servidores o componentes de servidores desde un recurso compartido de red mediante la integración de los chasis modulares Dell Repository Manager y Dell PowerEdge FX2/FX2s simplifica la actualización mediante el paquete de firmware personalizado para que pueda realizar implementaciones de manera más sencilla y rápida. Actualizar desde un recurso compartido de red proporciona flexibilidad para actualizar todos los componentes del servidor de 12a generación al mismo tiempo con un solo catálogo desde un CIFS o NFS.

Este método proporciona una forma rápida y sencilla de crear un repositorio personalizado para sistemas conectados de su propiedad 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 incluya 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 tener la licencia iDRAC Enterprise
- Lifecycle Controller debe estar activado en los servidores.
- 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 de la 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 de la CMC, en el árbol del sistema, vaya a **Visión general del servidor** y, a continuación, haga clic en **Actualizar** > **Actualización de 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 Elección de tipo de actualización de firmware para 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 paquetes personalizados de actualizaciones. Este Repository se almacena en el recurso compartido de CIFS o NFS que configura la CMC. Para obtener información sobre la creación de un repositorio mediante Dell Repository Manager, consulte la *Guía del usuario de Dell Repository Manager Data Center versión 1.8* y *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 los componentes y los dispositivos para la ranura específica. Como alternativa, para volver a ver todos los detalles, 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: La columna Estado de trabajo muestra el estado de las operaciones programadas en el servidor. El estado de trabajo se actualiza de forma dinámica.

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.

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
- Todos los servidores y los servidores individuales
- IO Modules (Módulos de E/S)
- Ventiladores
- Unidades de suministro de energía (PSU)
- Sensores de temperatura
- Dispositivos PCIe
- SLED de almacenamiento

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, la CMC, los módulos de los servidores, los módulos de I/O (IOM), los ventiladores, las fuentes de alimentación (PSU), los sled 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 *Guía del usuario de Integrated Dell Remote Access Controller (iDRAC)*.

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, posterior y superior de las imágenes que están más arriba o más abajo, respectivamente. Los servidores y los KVM 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) 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, aparecen datos sobre herramientas con información adicional acerca de ese componente.

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

Imagen	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.

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

Imagen	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.

NOTA: De manera predeterminada, los iconos de estado del servidor para 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 rápidos: proporciona vínculos para navegar a las páginas de acceso más frecuente y también a las acciones que se realizan con mayor frecuencia. En esta sección, solo se muestran vínculos aplicables al componente seleccionado.

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

NOTA: En Administración de varios chasis (MCM), no se muestran todos los **vínculos rápidos** asociados con los servidores.

Tabla 13. Propiedades de los componentes

Componente	Propiedades de condición y rendimiento	Propiedades	Vínculos de acceso rápido
CMC	• Dirección MAC • IPv4 • IPv6	• Firmware • Última actualización • Hardware	• Estado de la CMC • Sistemas de red • Actualización del firmware
Todos los servidores y servidores individuales	• Estado de la alimentación • Consumo de alimentación • Estado • Energía asignada • Temperatura	• Nombre • Modelo • Etiqueta de servicio • Nombre del host • iDRAC • CPLD • BIOS • SO • Información de la CPU • Memoria total del sistema	• 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 de Apagar servidor y Apagado ordenado se muestran solo si el estado de la alimentación del servidor es Encendido. Si el estado de la alimentación del servidor es Apagado, en su lugar aparece el vínculo rápido para Encender servidor.

Todos los SLED de almacenamiento y almacenamiento individual	Estado	• Nombre
		• Modelo
		• Etiqueta de servicio
		• Etiqueta de activo
		• Número de controladoras
		  ○ Ranuras de discos físicos
		  ○ Conectado al servidor
		  ○ Capacidad de modo de la controladora
		• Estado de intrusión
			• Estado del arreglo de almacenamiento
			• Configuración de la matriz de almacenamiento

Fuentes de alimentación	Estado de la alimentación	Capacidad	• Estado del suministro de energía • Consumo de alimentación • Presupuesto del sistema
Dispositivos PCIe	• Inlstalada • Asignada	• Modelo • Asignación • Id. de vendedor • Id. de dispositivo	• Estado de PCIe • Configuración de PCIe

Tabla 13. Propiedades de los componentes (continuación)

Componente	Propiedades de condición y rendimiento	Propiedades	Vínculos de acceso rápido
		• Tipo de ranura • Tipo de módulo • Red Fabric • Estado de la alimentación	
Ventiladores	• Velocidad • PWM (% del máximo) • Desplazamiento del ventilador	• Umbral de aviso • Umbral crítico	• Estado de los ventiladores • Configuración del ventilador
Ranura del módulo de E/S	• Estado de la alimentación • Rol	• Modelo • Etiqueta de servicio	Estado 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 una ranura, la imagen correspondiente en el gráfico aparecerá atenuada.
2. Coloque 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 nombre de modelo del almacenamiento y de la etiqueta de servicio

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

1. En el panel izquierdo, bajo el nodo de árbol **Descripción general del servidor**, aparecen todos los sleds de almacenamiento en la lista. Si un sled de almacenamiento no está presente en una ranura, la imagen correspondiente en el gráfico aparece atenuada.
2. Coloque el cursor en el número de ranura del sled de almacenamiento.
   La información sobre herramientas, si está disponible, muestra el nombre de modelo y la etiqueta de servicio del sled de almacenamiento.

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 acerca de esta página, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

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 **Estado de la controladora del chasis**. Para obtener más información, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

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** muestra una descripción gráfica de todos los servidores instalados en el chasis. El estado del servidor se indica mediante la superposición del subgráfico del servidor. Para obtener más información sobre el estado del chasis, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.
- 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 los sled de almacenamiento

Para ver el estado de la condición de los sled de almacenamiento:

En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del servidor**y seleccione el sled de almacenamiento.
La página **Estado de arreglo de almacenamiento** muestra las propiedades del sled de almacenamiento y la lista de nodos de almacenamiento conectados al sled de cálculo. Para obtener más información, consulte la *Ayuda en línea*.

Visualización de la información y del estado de la condición de los módulos 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 posterior, frontal y superior del chasis y contienen el estado del módulo de E/S. Dicho estado se indica mediante la superposición del subgráfico del módulo de E/S. 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 de la CMC para Dell PowerEdge FX2/FX2s*.

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 inicia 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; para ello, aumenta o disminuye la velocidad del ventilador según los eventos del sistema. Puede ejecutar el ventilador en tres modos como, por ejemplo, Bajo, Medio y Alto (intervalo del ventilador). Para obtener más información sobre cómo configurar un ventilador, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

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 *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2/FX2s* disponible en dell.com/support/manuals.

NOTA: La CMC supervisa los sensores de temperatura en el chasis y ajusta automáticamente la velocidad del ventilador según sea necesario. 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. Sin embargo, puede realizar un reemplazo para mantener una velocidad mínima del ventilador mediante el comando `fanoffset` de RACADM.

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, algunas o todas las unidades de los ventiladores en el chasis giran 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 posterior derecha de los gráficos del chasis ofrece la vista superior 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 más 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: esta función le permite aumentar el suministro de flujo de aire a las ranuras de tarjetas de 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 del ventilador (aumento) del 20%, 50% y 100% de la velocidad máxima respectivamente. También se puede configurar una velocidad mínima para cada opción, que es de 35% para Bajo, 65% para Medio y 100% para Alto. Sin embargo, en función de la configuración, el mínimo de velocidad para las opciones Bajo, Medio y Alto podría ser mayor que estos valores.

Por ejemplo, si se utiliza la configuración de desplazamiento del ventilador medio, se aumenta la velocidad de los ventiladores a un 50% de su velocidad máxima. Este aumento supera la velocidad de enfriamiento ya establecida por el sistema en función de la configuración del hardware instalado.

Con cualquiera de las opciones de Desplazamiento del ventilador activadas, aumenta el nivel de consumo de energía. El sistema es más ruidoso con el desplazamiento Bajo, mucho más ruidoso con el desplazamiento Medio y significativamente más 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** de la lista desplegable **Valor**, correspondiente al **Desplazamiento del ventilador**, seleccione la opción adecuada.

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>]
```

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 KVM**
   - **Indicadores del panel frontal**

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:

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 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 **Visión 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.

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 los valores de configuración de red de la misma para que pueda administrarse de manera remota. Esta configuración inicial asigna los parámetros de red TCP/IP que permiten tener acceso a la CMC.

Es posible configurar la CMC por medio de la interfaz web o la Configuración del acceso inicial a RACADM de CMC.

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.
- 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.
- Agregue y configure los sled de almacenamiento.

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:

Activación o desactivación de DHCP para la dirección de interfaz de red de la 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 forma predeterminada.

Puede activar el DHCP para obtener de forma automática una dirección IP desde el servidor DHCP.

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 activar 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 1
```

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 1
```

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>
```

Visualización y modificación de la configuración de red LAN de la 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.

Cuando IPv6 se activa en el momento del inicio, se envían tres solicitudes de enrutador cada cuatro segundos. Si los conmutadores de red externos ejecutan el Protocolo de árbol de expansión (STP), es posible que los puertos de los conmutadores externos queden bloqueados durante un plazo mayor a los doce segundos en los que se envían las solicitudes de enrutador IPv6. En esos casos, es posible que exista un período en el que la conectividad de IPv6 sea limitada, hasta que los enrutadores IPv6 envíen los anuncios de enrutador sin ser requerido.

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 de la CMC mediante la interfaz web de la 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 de la configuración de red LAN de la CMC mediante RACADM

Para ver la configuración de IPv4, utilice el objeto `cfgCurrentLanNetworking` con los siguientes subcomandos:

- `getniccfg`
- `getconfig`

Para ver la configuración de IPv6, utilice `cfgIpv6LanNetworking` con el subcomando `getconfig`.

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

Para obtener más información acerca de los objetos y subcomandos, consulte *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2/FX2s*.

Activación de la interfaz de red de la 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:

Si desactiva la interfaz de red de la CMC, la operación de desactivación realiza las siguientes acciones:

- Desactiva el acceso a la interfaz de red para la administración fuera de banda, incluso la adminstración del iDRAC y del módulo de E/S.
- Evita la detección de estado del enlace descendente.

  Para desactivar solo el acceso a la red de la CMC, desactive la IPv4 de la CMC y la IPv6 de la CMC.

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: El direccionamiento IPv6 de la CMC está desactivado de forma predeterminada.

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>
```

El DHCP está desactivado de forma predeterminada. Para habilitarlo y utilizar el servidor de DHCP en la red y así poder asignar la dirección IPv4 de la CMC o del iDRAC, la máscara de subred y puerta de enlace, escriba:

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

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>
```

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 del dominio DNS**: el nombre predeterminado del dominio DNS es un único carácter 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 la CMC debe establecer automáticamente el modo dúplex y la velocidad de la red mediante la comunicación con el enrutador o el conmutador más cercano. La negociación automática está activada de forma predeterminada.

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 del puerto de administración 2

El segundo puerto de red de la CMC se puede utilizar para la conexión en cadena de las CMC con motivo de reducción de cables, o como un puerto redundante para la operación de redes de conmutación por error. El **Puerto de administración 2** pueden estar conectado al conmutador de la parte superior del bastidor (TOR) o a otro conmutador. No es necesario conectar los dos puertos NIC de la CMC a la misma subred.

La CMC no se puede instalar para redundancia de Puertos de la red de administración antes de configurarla realmente para esta operación. La CMC debe utilizar la conexión de red única estándar para la implementación, después de la cual se puede realizar la segunda conexión redundante.

NOTA: Si el Puerto de administración 2 está configurado para la redundancia pero está cableado para el apilamiento, las CMC descendentes (desde el conmutador TOR) no tendrán vínculo de red.

NOTA: Cuando el Puerto de administración 2 está configurado para el apilamiento pero está cableado para la redundancia (dos conexiones al conmutador TOR), los bucles de enrutamiento causarán un inconveniente de red.

Para especificar la operación redundante, utilice el comando `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 1`.

Para especificar la operación de apilamiento, utilice el comando `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 0`.

De manera predeterminada, el puerto de administración 2 está configurado para el apilamiento.

Configuración del puerto de administración 2 mediante la interfaz web de la CMC

Para configurar el puerto de administración mediante la interfaz web de la CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Red**y, a continuación, haga clic en la ficha **Red** .
2. En la página **Configuración de la red**, en la sección **Configuración general**, junto a **Puerto de administración 2**, seleccione **Redundante** o **Apilamiento**.
3. Haga clic en **Aplicar cambios**.

- Cuando el Puerto de administración 2 está configurado como Redundante pero está cableado para Apilamiento, las CMC de bajada (desde el conmutador de la parte superior del bastidor) no tendrán un vínculo de red.
- Cuando el Puerto de administración 2 está configurado para el apilamiento pero está cableado para la redundancia (dos conexiones al conmutador TOR), los bucles de enrutamiento causarán un inconveniente de red.

Configuración del puerto de administración 2 mediante RACADM

Para especificar la operación redundante, utilice el comando `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 1`.

Para especificar la operación de apilamiento, utilice el comando `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 0`.

De manera predeterminada, el puerto de administración 2 está configurado para el apilamiento.

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. La 140-2 consta de cuatro niveles: nivel 1, nivel 2, nivel 3 y nivel 4. La serie FIPS 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 *Ayuda en línea para el 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 **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 remoto: active el acceso a la 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.

NOTA: Al modificar los números del puerto de servicio de la CMC para SSH, Telnet, HTTP o HTTPS, evite usar puertos utilizados comúnmente por los servicios del SO, como puerto 111. Consulte los puertos reservados por la Internet Assigned Numbers Authority (IANA) en http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

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 remoto requieren este servicio para comunicarse con la CMC.

Si se restablece el servidor web, espere por lo menos un minuto para que los servicios estén nuevamente disponibles. El restablecimiento del servidor web generalmente se produce 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 destinos correspondientes.

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.

Los puertos de red reservados para comunicaciones de la CMC y del iDRAC son 21, 68, 69, 123, 161, 546, 801, 4003, 4096, 5985 a 5990, 6900 y 60106.

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 la *Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge FX2/FX2s* 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, el uso de RACADM para habilitar el registro del sistema remoto en un iDRAC no admitido muestra un mensaje de error.

De forma similar, cuando se muestran las propiedades del iDRAC con el uso del 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 de la CMC

Es posible activar o reparar los medios flash extraíbles opcionales para utilizarlos como 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 acerca de estas opciones, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.
3. Haga clic en **Aplicar** para aplicar la opción seleccionada.

Configuración de un grupo de chasis

La CMC le permite monitorear 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 de las condiciones del chasis principal y de los miembros de un grupo se marcan con superposiciones rojas o amarillas y 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 del chasis o en **Detalles**.
- Los vínculos de inicio rápido están disponibles para abrir las páginas web de los servidores 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 19 miembros. Asimismo, un chasis principal o miembro solo puede participar de un grupo. No puede unirse a un chasis como principal o miembro que 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 **Rol**, seleccione **Principal**. Aparecerá un campo para agregar el nombre del 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 del chasis, la interfaz gráfica de usuario cambia 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.

   NOTA: Cuando se crea un grupo de chasis, el elemento **Descripción general del chasis** en la estructura de árbol se reemplaza por el nombre del chasis principal.

Adición de miembros a un grupo de chasis

Una vez configurado el grupo de chasis, agregue miembros al grupo mediante los siguientes pasos:

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**.

   NOTA: Para que MCM funcione correctamente, debe utilizar el puerto HTTPS predeterminado (443) en todos los miembros de grupo y el chasis principal.

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. Para obtener más información acerca de cómo agregar miembros al grupo del chasis, consulte Sincronización de un miembro nuevo con las propiedades del chasis principal.
8. Haga clic en **Aplicar**.
9. Para agregar un máximo de 19 miembros, lleve a cabo las tareas en los pasos del 4 al 8. Los nombres de chasis de los nuevos miembros aparecen en el cuadro de diálogo **Miembros**.

   NOTA: Las credenciales introducidas para un miembro se envían de manera segura al chasis miembro para establecer una relación de confianza entre el chasis principal y el miembro. Las credenciales no se conservan en ninguno de los dos 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 comunicará al miembro o los miembros, si se selecciona más de uno, que se lo ha eliminado del grupo. Se ha eliminado 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**.

   Posteriormente, el chasis principal comunica a todos los miembros que han sido eliminados del grupo. El chasis principal se puede asignar como chasis principal o chasis miembro de un grupo nuevo.

   Si un problema de red evita el contacto entre el chasis principal y el chasis miembro, este último puede no recibir el mensaje. En ese caso, desactive el miembro del chasis miembro para poder quitarlo totalmente.

Desactivación de un miembro individual del chasis miembro

En ocasiones, no se puede eliminar un miembro de un grupo mediante el chasis principal. Esto puede ocurrir 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**.

Inicio de 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 del 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: El Inicio de sesión único y el Inicio de sesión mediante tarjeta inteligente no se admiten en la Administración de varios chasis. Para ejecutar los miembros mediante el inicio de sesión único desde el chasis principal se requiere un nombre de usuario/contraseña común entre el chasis principal y los chasis miembros. El uso de un nombre de usuario/contraseña común funciona solo 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 intenta iniciar sesión en el chasis miembro mediante **Iniciar CMC** cuando ambos chasis, el principal y el miembro, están activados o desactivados para FIPS, se lo redirigirá a la página **Condición del grupo del chasis**. De lo contrario, se lo redirigirá a la página **Inicio de sesión** del chasis miembro.

   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 la casilla etiquetada **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 muestra ninguno de 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 cambien las propiedades del chasis principal.
- Propagación manual: seleccione esta opción para propagar manualmente las propiedades del chasis principal del grupo a sus miembros. La configuración de las propiedades del chasis principal se propaga a los miembros del grupo solo cuando un 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 de configuración que desea que se configuren de manera 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 alerta 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*.

Sincronización de un miembro nuevo con las propiedades del chasis principal

Puede aplicar las propiedades del chasis principal a un chasis miembro de un grupo recientemente agregado. Para sincronizar un nuevo miembro con las propiedades del chasis principal:

1. Inicie sesión en el chasis principal con privilegios de administrador.
2. Seleccione el chasis principal en la estructura de árbol.
3. Haga clic en **Configuración** > **Administración de grupos**.
4. Al agregar un miembro nuevo al grupo, en la página **Grupo de chasis**, seleccione **Sincronizar el miembro nuevo con las propiedades del principal**.
5. Haga clic en **Aplicar**. El miembro adquirirá las propiedades del principal.

La sincronización afecta las siguientes propiedades del servicio de configuración de varios sistemas en el chasis:

Tabla 14. Propiedades del servicio de configuración

Propiedad	Navegación
Configuración de SNMP	En el panel izquierdo, haga clic en **Descripción general del chasis** > **Red** > **Servicios** > **SNMP**.
Registro remoto del chasis	En el panel izquierdo, haga clic en **Descripción general del chasis** > **Red** > **Servicios** > **Syslog remoto**.
Autentificación de usuario con LDAP y Active Directory	En el panel izquierdo, haga clic en **Descripción general del chasis** > **Autentificación de usuario** > **Servicios de directorio**.
Alertas del chasis	En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, haga clic en **Alertas**.

Inventario del servidor para el grupo de MCM

Un grupo es un chasis principal que contiene entre 0 y 19 miembros de grupo de chasis. 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).
- Ranuras vacías y de extensión.

Cómo 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.

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 *Ayuda en línea para el CMC*.

Cómo importar perfiles de configuración del chasis

Puede importar perfiles de configuración del chasis almacenados en un recurso compartido de red a la estación de administración local.

Para importar un perfil almacenado en un recurso compartido de archivos remotos a la CMC, realice las siguientes tareas:

1. Diríjase a la página **Perfiles de configuración del chasis**. En la sección **Perfiles de configuración del chasis** > **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**.

NOTA: Puede importar perfiles de configuración del chasis mediante RACADM. Para obtener más información, consulte la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e*.

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. Vaya 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**.
   Se mostrará el mensaje `Operation Successful`.
3. Haga clic en **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 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>
```

Configuración de varias CMC mediante RACADM

Por medio de RACADM, es posible configurar uno o varios CMC con propiedades idénticas.

Cuando 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` de la información recuperada. Al exportar el archivo a una o varias CMC, es posible configurar sus controladoras con propiedades idénticas en una cantidad de tiempo mínima.

NOTA: Algunos archivos de configuración contienen información exclusiva del CMC (como la dirección IP estática) que se debe modificar antes de exportar el archivo a otros CMC.

1. Use RACADM para hacer una consulta en el CMC de destino que contiene la configuración deseada.

   NOTA: El archivo de configuración generado es `myfile.cfg` Puede cambiar el nombre del archivo. El archivo `.cfg` generado no contiene contraseñas de usuario. Cuando el archivo `.cfg` se carga en la nueva CMC, es necesario volver a agregar todas las contraseñas.

2. Abra una consola de texto de Telnet/SSH en la CMC, inicie sesión y 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 textos sin formato (opcional). Todo 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 para la CMC y genera el archivo `myfile.cfg`. De ser 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 del usuario y la contraseña.

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 modernos podrían incluir caracteres '#' en su cadena. No se requiere un carácter de escape. Es posible que desee 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 encontrarse 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 según se define en el capítulo de propiedad de base de datos de la *Guía de referencia de la línea de comandos de RACADM para iDRAC y CMC*. 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 continúa sin modificación. Cualquier carácter que se encuentre a la derecha del signo = (por ejemplo, un segundo signo =, #, [,], etc.) se tomará tal como se encuentre. Estos son caracteres válidos de secuencia de comandos del chat del módem.

  ```
  [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 1-16> <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 1-16> ""
  ```

  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 1-16>
```

- Para los grupos indexados, el ancla del objeto debe ser el primer objeto después del par [ ]. Los siguientes son 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 de un 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 de la CMC

Cuando modifique la dirección IP de la CMC en el archivo de configuración, elimine todas las entradas `<variable> = <value>` innecesarias. Solo la etiqueta del grupo variable real con [y] permanecerá, incluidas las dos entradas `<variable> = <value>` relacionadas con el cambio en la dirección IP.

Por ejemplo:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=192.x.x.x
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`.

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 VLAN de 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 32 a 126). También se permite el uso de caracteres estándares y especiales en los nombres.
- Los nombres de las ranuras deben ser únicos dentro del chasis. Las ranuras no pueden 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-`
  - `Chassis`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- Las cadenas del `Server-1` al `Server-4` se pueden utilizar únicamente 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**.

La configuración de cada nombre de ranura en la interfaz web se encuentra únicamente en la CMC. Si un servidor se retira del chasis, la configuración de los nombres de las ranuras no permanecerá 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 de un servidor como nombre de ranura, seleccione la opción **Utilizar nombre de host para el nombre de las ranuras** . Esto suprime los nombres de ranura estáticos con el nombre de host del servidor (o el nombre del sistema), si se encuentra disponible. Para ello, el agente de OMSA debe estar instalado en el servidor. Para obtener más información sobre el agente de OMSA, consulte la *Guía del usuario de OpenManage Server Administrator de Dell,*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 las ranuras**. 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 ranura 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-4) según la posición de la ranura del 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 la red del iDRAC de un servidor. Puede usar la configuración de QuickDeploy para configurar los ajustes 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 el iDRAC, consulte la *DRAC 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 página **Implementar iDRAC**, 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 15. 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. • **QuickDeploy solamente**: seleccione esta opción para aplicar la configuración de red del iDRAC cuando se inserta un nuevo servidor en el chasis. La configuración de implementación automática especificada se usa para configurar el nuevo iDRAC, lo cual incluye 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 de servidor**: seleccione esta opción para aplicar primero la configuración de red del iDRAC y, a continuación, el perfil de 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 de 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 un chasis. La contraseña puede tener de 1 a 20 caracteres imprimibles (incluidos espacios en blanco).

Tabla 15. Configuración de QuickDeploy (continuación)

Configuración	Descripción
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 de iDRAC. De manera predeterminada, se desmarca esta opción.
Activar IPv4 del iDRAC	Activa o desactiva IPv4 en iDRAC. De manera predeterminada, esta opción está seleccionada.
Activar la IPMI en la LAN del iDRAC	Activa o desactiva el canal IPMI en la LAN para cada iDRAC presente en el chasis. De manera 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 opción de dirección IP de QuickDeploy se proporcion con dos valores 4 y 2.
Dirección IP de QuickDeploy reservada	Seleccione la cantidad de direcciones IPv4 estáticas reservadas para los iDRAC en el chasis. Las direcciones IPv4 que se inician de **Dirección IPv4 inicial del iDRAC (ranura 1)** se consideran reservadas y se asume que se encuentran sin usar en otra ubicación de la misma red. QuickDeploy no funciona en servidores que se han insertado en ranuras para las cuales no existe ninguna dirección IPv4 estática reservada.
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 4c es `192.168.0.265`. Si la máscara de subred es `255.255.255.0`, se muestra el mensaje de error `QuickDeploy IP address range is not fully within QuickDeploy Subnet` cuando hace clic en **Guardar configuración de QuickDeploy** o en **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.
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 habilitada.
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	Activa los valores de configuración del servidor DNS de la CMC (IPv4 e IPv6) que se propagan al iDRAC cuando se inserta un servidor blade en el chasis.
Habilitar el nombre DNS de iDRAC	Seleccione **Habilitar el nombre DNS de iDRAC** para aplicar el nombre DNS de iDRAC a los servidores blade insertados en el chasis. Puede ingresar el prefijo de DNS de iDRAC, que la CMC agrega al nombre de ranura. Por ejemplo, si el prefijo de DNS de iDRAC es "DNSNAME", el nombre de DNS de iDRAC se anexa al nombre de ranura, "DNSNAME-SlotN".

Tabla 15. Configuración de QuickDeploy (continuación)

Configuración	Descripción
	De manera predeterminada, Habilitar el nombre DNS de iDRAC está deshabilitado.
Nombre DNS de iDRAC (prefijo)	Puede configurar el prefijo del nombre DNS de iDRAC solo si selecciona Habilitar el nombre DNS de iDRAC. El prefijo del nombre DNS puede contener un máximo de 59 caracteres y un carácter como mínimo. Los caracteres admitidos son los siguientes: ● Alfanuméricos: "a-b" o "A-B" ● Numéricos: "0-9" ● Guion: "–" Asegúrese de que el prefijo del nombre DNS no comience con un guion. El prefijo predeterminado es "idrac". Solo el prefijo del nombre DNS de iDRAC se almacena en el perfil del servidor.

3. Haga clic en **Guardar configuración de QuickDeploy** para guardar la configuración. Si cambió la configuración de red de iDRAC, haga clic en **Aplicar configuración de red de iDRAC** para implementar la configuración en iDRAC.

   La función QuickDeploy solamente se ejecuta cuando está activada y se inserta un servidor en el chasis.

   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 que se realizan en los campos de QuickDeploy son inmediatos, pero los cambios realizados a uno o más ajustes de configuración de red del servidor iDRAC pueden tardar unos minutos en propagarse de la CMC al iDRAC. Si hace clic en **Actualizar** demasiado pronto, es posible que solo aparezcan datos parcialmente correctos para uno o más servidores iDRAC.

Asignación de direcciones IP de QuickDeploy para servidores

Las tablas siguientes muestran la forma en que se asignan las direcciones IP de QuickDeploy a los servidores en función de los sleds presentes en el chasis FX2/FX2s:

- Dos sleds de ancho completo en el chasis:

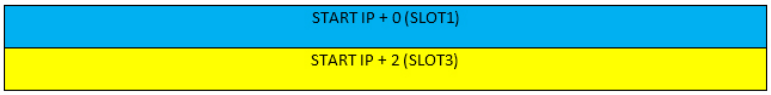


Ilustración 3. Dos sleds de ancho completo en el chasis

- Cuatro sleds de mitad de ancho en el chasis:

Ilustración 4. Cuatro sleds de mitad de ancho en el chasis

- Ocho sleds de cuarto de ancho en el chasis:

  NOTA: La opción **Direcciones IP de QuickDeploy reservadas** debe establecerse, como mínimo, en 8.

Ilustración 5. Ocho sleds de cuarto de ancho en el chasis

- Cuatro sleds FM120x4 en el chasis:

  NOTA: La opción **Direcciones IP de QuickDeploy reservadas** debe establecerse en 16.

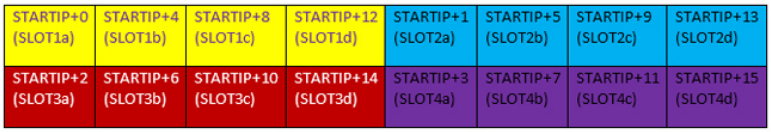


Ilustración 6. Cuatro sleds FM120x4 en el chasis

- La fila superior contiene solo sleds de cuarto de ancho y la fila inferior contiene solo sleds de mitad de ancho:

  NOTA: La opción **Direcciones IP de QuickDeploy reservadas** debe establecerse, como mínimo, en 8.

Ilustración 7. Sleds de cuarto de ancho en la fila superior y sleds de mitad de ancho en la fila inferior

- La fila superior contiene solo sleds de ancho completo y la fila inferior contiene solo sleds de mitad de ancho:

Ilustración 8. Sleds de ancho completo en la fila superior y sleds de mitad de ancho en la fila inferior

- La fila superior contiene solo sleds de ancho completo y la fila inferior contiene solo sleds de cuarto de ancho:

  NOTA: La opción **Direcciones IP de QuickDeploy reservadas** debe establecerse, como mínimo, en 8.

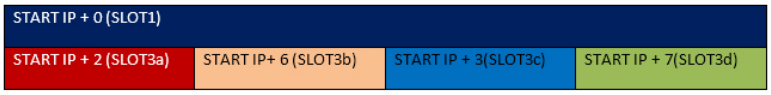


Ilustración 9. Sleds de ancho completo en la fila superior y sleds de cuarto de ancho en la fila inferior

Modificación de la configuración de red del iDRAC en un servidor iDRAC individual

Con esta función, puede configurar los ajustes de configuración de red iDRAC para cada servidor instalado. Los valores iniciales que se muestran para cada uno de los campos 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, luego, haga clic en **Configuración**. En la página **Implementar iDRAC**, en la sección **Configuración de red de iDRAC** se muestra el nombre de DNS del iDRAC y los ajustes de configuración de red IPv4 e IPv6 de todos los servidores instalados.
2. Modifique la configuración de red del iDRAC según sea necesario para los servidores.

   NOTA: Debe seleccionar la opción **Habilitar LAN** para especificar la configuración de IPv4 o IPv6. Para obtener información sobre los campos, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.

3. Para implementar la configuración en iDRAC, haga clic en **Aplicar configuración de red de iDRAC**. También se guardan los cambios realizados en la **configuración de QuickDeploy**.

   En la tabla **Configuración de red de iDRAC**, se reflejan los futuros ajustes de configuración de red. Los valores que se muestran para los servidores instalados pueden ser los mismos que los ajustes de configuración de red iDRAC instalados actualmente. Haga clic en **Actualizar** para actualizar la página **Implementar iDRAC** en cada uno de los ajustes de configuración de red iDRAC instalados después de realizar cambios.

   NOTA: Los cambios que se realizan en los campos de QuickDeploy son inmediatos, pero los cambios realizados a uno o más ajustes de configuración de red del servidor iDRAC pueden tardar unos minutos en propagarse de la CMC al iDRAC. Si hace clic en **Actualizar** demasiado pronto, es posible que solo aparezcan datos parcialmente correctos para uno o más servidores 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 rangos predeterminados de la propiedad, consulte la *Guía de referencia de la línea de comandos RACADM de Integrated Dell Remote Access Controller* y la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2/FX2s* disponibles en **dell.com/support/manuals**.

Configuración de los valores de las etiquetas VLAN para el iDRAC

Las VLAN se utilizan para permitir que varias LAN virtuales 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 aún cuando se elimina un componente.

NOTA: La configuración de VLAN del iDRAC desde la CMC se aplica solo cuando la selección de la NIC del iDRAC está establecida en el modo LOM (dedicada) de iDRAC para el chasis.

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 el modo LOM compartido, los cambios de la ID de VLAN realizados en el iDRAC no se muestran en la interfaz gráfica de usuario del CMC.

Configuración de los valores de la etiqueta VLAN del iDRAC mediante la interfaz web

Para configurar VLAN para servidores:

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 la red VLAN para los servidores, establezca la prioridad y especifique la ID. Para obtener información sobre los campos, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.
3. Haga clic en **Aplicar** para guardar la configuración.

Configuración de los valores de la etiqueta VLAN del iDRAC mediante RACADM

- Especifique la identificación y la prioridad de VLAN 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 16.

Por ejemplo:

```
racadm setniccfg -m server-1 -v
```

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 para el servidor o incluso puede no representar a un dispositivo existente en ese servidor. Representa un dispositivo enviado por la CMC al servidor y utilizado como primer dispositivo de inicio de ese servidor. Este dispositivo se puede establecer como primer dispositivo de inicio predeterminado o dispositivo de inicio por una única 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. El usuario también puede especificar el primer dispositivo de inicio para el servidor. El sistema se inicia desde el dispositivo seleccionado en los próximos inicios y permanece como el primer dispositivo de inicio en el orden de inicio del BIOS, hasta que se cambie de nuevo desde la interfaz web de la CMC 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. Sin embargo, para configurar un dispositivo como primer dispositivo de inicio predeterminado, seleccione **Predeterminado**.

Para no omitir la versión de firmware del servidor si la versión del firmware que se ejecuta en el servidor es la misma que la versión disponible en el primer dispositivo de inicio, seleccione **Ninguno**.

Es posible establecer los siguientes dispositivos para el primer inicio.

Tabla 16. 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 mediante una unidad de disco duro.
CD/DVD local	Inicio a partir de una unidad de CD/DVD en el servidor.
Configuración del BIOS	Inicio durante la configuración del BIOS.
Disco flexible virtual	Inicio desde un disco flexible virtual.
CD/DVD virtual	Inicio desde una unidad de DVD o de CD virtual.
Tarjeta SD local	Inicio desde la tarjeta SD (Secure Digital) local.
Recurso compartido de	Inicio desde el recurso compartido de archivos remotos.

Tabla 16. Dispositivos de inicio (continuación)

Dispositivo de inicio	Descripción
archivos remotos	
Administrador de inicio del BIOS	Inicio mediante el administrador de inicio del BIOS.
Lifecycle Controller	Inicio mediante Lifecycle Controller.
Disco flexible local	Inicio a partir de un disco flexible en la unidad de disco flexible local.

Configuración del primer dispositivo de inicio para varios servidores mediante la interfaz web de la 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** > **Dispositivo de primer 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 **Iniciar una vez**. Si desea que el servidor utilice el dispositivo seleccionado solo en el siguiente ciclo de inicio, seleccione la opción **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 de la 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 **Iniciar una vez**. Si desea que el servidor utilice el dispositivo seleccionado solo en el siguiente ciclo de inicio, seleccione la opción **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 la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2s* disponible en dell.com/support/manuals.

Configuración del vínculo ascendente de red del sled

Puede configurar el vínculo ascendente de red del sled solo en los sleds de PowerEdge FM120x4 que contienen un conmutador de red interno.

Para configurar el vínculo ascendente de red del sled, vaya a **Descripción general del chasis** > **Descripción general del servidor** > **Configurar** > **Vínculo ascendente de red del sled**

Seleccione uno de los siguientes valores para la propiedad de configuración del vínculo ascendente de red del sled:

- **Estándar (agregado)**: configuración de vínculo ascendente donde los cuatro puertos del vínculo ascendente del módulo de E/S están configurados en un solo grupo troncal y todos los LOM están asignados a dicho grupo. Esta opción está seleccionada de manera predeterminada.
- **Aislamiento del adaptador de red (seguridad mejorada)**: configuración de vínculo ascendente similar a la estándar, pero no se permite el enrutamiento entre nodos locales.
- **Redes aisladas**: configuración de vínculo ascendente donde el LOM1 de cada nodo se asigna al módulo de E/S A1 y el LOM2 se asigna al módulo de E/S A2.
- **Aislamiento mejorado del adaptador de red**: configuración de vínculo ascendente para mejorar la seguridad en las configuraciones de varios usuarios. Esta configuración aísla los adaptadores de red individuales con un puerto M. E/S dedicado y asignado al LOM de cada nodo. Solo el LOM1 en cada nodo está operativa.

NOTA: Al ir de la CMC versión 1.3 o posterior a una anterior, si la **Configuración de vínculo ascendente de red del sled** se establece en **Aislamiento mejorado del adaptador de red**, la **Configuración de vínculo ascendente de red del sled** aparece en blanco en la CMC 1.2 o versiones anteriores. En la CLI, el valor no válido '4' se muestra como la salida para el comando:

```
$ getconfig -g cfgRacTuning -o cfgRacTuneSledNetworkUplink
```

Implementación de un recurso compartido de archivos remoto

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 de manera 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.

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 más información sobre las descripciones de los campos, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.
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 FlexAddress para el servidor

Para obtener información acerca de cómo configurar FlexAddress para servidores, consulte Configuración de FlexAddress para redes Fabric y ranuras en el nivel del chasis mediante la interfaz web de la CMC. Para usar esta función, debe tener una licencia Enterprise.

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 configuraciones de perfil de un servidor especificado a uno o más servidores. Las configuraciones 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 para servidores, los cuales pueden replicarse:

- BIOS: este grupo incluye solo los valores del BIOS de un servidor.
- BIOS e inicio: este grupo incluye los valores del BIOS y de inicio de un servidor.
- Todas las configuraciones: esta versión incluye todas las configuraciones del servidor y los componentes en ese servidor. Estos perfiles se generan desde:
  - Servidores de 12.ª generación con iDRAC7 1.57.57 o posterior y Lifecycle Controller 2 versión 1.1 o posterior
  - Servidores de 13.ª generación con iDRAC8 2.05.05 con Lifecycle Controller 2.00.00.00 o posterior.

La función de clonación de servidores admite los servidores iDRAC7 e iDRAC8. Los servidores RAC de generaciones anteriores se muestran en la lista pero aparecen en gris 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. Los servidores iDRAC7 requieren la versión 1.57.57. Los servidores iDRAC8 requieren la versión 2.05.05.
- 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.

Cómo acceder a la página Perfil

Es posible agregar, administrar y aplicar perfiles en uno o varios servidores mediante la página **Perfil**.

Para acceder a la página **Perfil** con el uso de la interfaz web de la CMC, en el panel izquierdo, haga clic en **Visión general del chasis** > **Visión general del servidor** > **Configuración** > **Perfiles**. Se muestra la página **Perfiles**.

Administración de perfiles almacenados

Es posible editar, ver o eliminar perfiles de BIOS. Para administrar los perfiles almacenados de una CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del servidor** > **Configuración** > **Perfiles**.
2. En la página **Perfiles**, en la sección **Aplicar perfil**, haga clic en **Administrar perfiles**. Se mostrará la página **Administrar perfiles de BIOS**.

- Para editar un perfil, haga clic en **Editar**.
- Para ver la configuración del BIOS, haga clic en **Ver**.

- Para eliminar un perfil, haga clic en **Eliminar**. Para más información sobre las descripciones de los campos, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

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 volátil 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, 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 a los perfiles almacenados y desactiva la función Clonación de servidores.

Para agregar un perfil:

1. Diríjase a 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 para 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, consulte Configuración de un recurso compartido de red mediante la interfaz web de la CMC.

4. En los campos **Nombre de perfil** y **Descripción**, introduzca el nombre de perfil y la descripción (opcional) y haga clic en **Guardar perfil**.

   NOTA:

   Al guardar un perfil de servidor, la lista de caracteres no admitidos para Nombre de perfil son hash (#), coma (,) y signo de interrogación (?).

   Se admite el conjunto de caracteres extendidos ASCII estándar. 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 clonación de servidores solo es posible cuando se dispone de perfiles de servidores como perfiles almacenados en los medios no volátiles de la CMC o almacenados en el recurso compartido remoto. Para iniciar una operación de clonación de servidores, puede aplicar un perfil almacenado a uno o más servidores.

El estado de la operación, el número de ranura, el nombre de ranura y el nombre de modelo de cada servidor se muestran en la tabla **Aplicar perfil**.

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 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 clasificados por tipo, incluidos aquellos que se encuentran en el repositorio 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 sobrescribe la configuración actual y también se reinician 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 la opción CSIOR está desactivada, se mostrará un mensaje de advertencia que indica que CSIOR no está activada 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 y estos se pueden reiniciar inmediatamente, de ser necesario. Para obtener más información, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

Importación de 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**, dentro de 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, consulte la *Ayuda en línea*.

Exportación de archivo

Puede exportar un perfil del servidor almacenado a una ruta 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 de advertencia que le indica que si 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, 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 de configuración del servidor normal (instantánea del servidor), que se puede utilizar para la replicación en un sistema de destino. Sin embargo, algunas configuraciones, como RAID y los atributos de identidad no se propagan al nuevo servidor. Para obtener más información sobre los modos exportación alternativos para las configuraciones RAID y los atributos de identidad, consulte el artículo, *Clonación de servidores con perfiles de configuración del servidor*, en **DellTechCenter.com**.

Edición de perfil

Puede editar el nombre y la descripción de un perfil de servidor que está almacenado en el soporte no volátil de la CMC (tarjeta de SD).

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 de BIOS — <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*.

Visualización de 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 de la 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, después de reiniciar el servidor, en la configuración de **F2**, seleccione **Configuración del iDRAC** > **Lifecycle Controller**, active **CSIOR** y guarde los cambios.

Para activar CSIOR en:

1. los servidores de 12.ª generación: después de reiniciar el servidor, en la configuración de F2 , seleccione **Configuración del iDRAC** > **Lifecycle Controller**, active **CSIOR** y guarde los cambios.
2. 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**.

Visualización de la configuración de los perfiles almacenados

Para ver la configuración de los perfiles de servidores almacenados, vaya a la página **Perfiles del servidor**. En la sección **Perfiles del servidor**, haga clic en **Ver** en la columna **Ver perfil** para el servidor requerido. Aparece la página **Ver configuración**. Para más información sobre la configuración que se muestra, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

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 clonación 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 las 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 de servidores, el cual se inserta 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 **Perfil de servidor** o en **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 el iDRAC**, seleccione **Descripción general del servidor** > **Configuración** > **iDRAC** . Todos los perfiles que pueden implementarse están en la tarjeta SD.

NOTA: Para configurar los perfiles para implementación rápida, debe tener privilegios de **Administrador del chasis**.

Asignación de perfiles del servidor a ranuras

La página **Perfiles del servidor** le permite asignar perfiles de servidor a ranuras. Para asignar un perfil a las ranuras del chasis:

1. En la página **Perfiles del servidor**, haga clic en **Perfiles para QuickDeploy.**
   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 selecciona esta opción, podrá 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 perfiles para aplicar a varias ranuras.
3. Haga clic en **Asignar perfil**.
   Se aplicará el perfil a las ranuras seleccionadas.

NOTA: Cuando se inserta el sled FM120x4, el perfil almacenado asignado a la ranura del servidor se aplica a los cuatro servidores.

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 una asignación de 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 la ranura se eliminan los valores de configuración XML en el perfil de los servidores insertados en las ranuras cuando se activa la función **Implementación rápida de perfiles**. 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 **Perfil para implementación rápida**, el progreso y los resultados de la aplicación se conservan en el registro de perfiles.

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*.

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 la configuración de los perfiles de identidad de inicio si los perfiles de identidad de inicio 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 solo 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 desea 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 identidad**.
3. Haga clic en **Aplicar identidad**.

   Aparece un mensaje de advertencia que indica que si se aplica una identidad nueva, se sobrescribirá la configuración actual y también se reiniciará 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 en el servidor, los servidores deben tener la opción CSIOR activada. Si la opción CSIOR está desactivada, aparece un mensaje de advertencia que indica que CSIOR no está activado 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 de inmediato. Para obtener más información, consulte *Ayuda en línea para el CMC*.

   NOTA: Puede aplicar un perfil de identidad de inicio para una sola partición de FQDD NIC en un servidor a la vez. Para aplicar el mismo perfil de identidad de inicio a una partición FQDD NIC en otro servidor, debe borrarla desde el servidor donde se había aplicado primero.

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 *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 *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 el 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 *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 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 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 iniciará sesión automáticamente en iDRAC mediante el inicio de sesión único. Una vez que se encuentre en el sitio del iDRAC, este usuario obtendrá privilegios de administrador automáticamente. Esto sucede incluso si el mismo usuario no dispone de una cuenta en el iDRAC o si la cuenta no tiene privilegios de administrador.
- Un usuario de la CMC que **NO** tenga privilegios de administración del servidor, pero tiene la misma cuenta en el iDRAC, iniciará sesión automáticamente en el iDRAC mediante el inicio de sesión único. Una vez que se encuentre en el sitio del iDRAC, este usuario obtendrá privilegios que fueron creados para la cuenta del iDRAC.
- Un usuario de la CMC que no tenga privilegios de administración del servidor, o de la misma cuenta en el iDRAC, no podrá iniciar sesión automáticamente en el iDRAC mediante el inicio de sesión único. Este usuario será dirigido a la página de inicio de sesión de iDRAC cuando se hace clic en **Iniciar 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 el CMC y el iDRAC. Se considera que un usuario que tiene el mismo nombre de inicio de sesión, pero con 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 interfaz gráfica de usuario del iDRAC**, puede aparecer una página de error, si:

- se quita un servidor del chasis.
- se modifica 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 misma. 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 **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 del servidor**, haga clic en **Iniciar interfaz gráfica de usuario del iDRAC**.
   Se muestra la interfaz web del iDRAC. Para obtener información sobre los campos, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

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 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 aparecen en la lista expandida de servidores.
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**.

NOTA: El botón o vínculo **Iniciar consola remota** se activa solo si el servidor tiene la licencia Enterprise instalada.

8

Configuración de sleds de almacenamiento

Los sleds de almacenamiento de medio ancho que se utilizan en el chasis FX2 contienen lo siguiente:

- Una o dos controladoras RAID
- Un máximo de 16 unidades de disco

Puede configurar los sleds de almacenamiento individuales que contienen dos controladoras RAID para que funcionen en los siguientes modos:

- Únido dividido
- Dual dividido
- Unido

NOTA: No inserte un sled de almacenamiento en la ranura 1 del chasis ya que esta no es una ubicación válida para los sleds de almacenamiento.

NOTA: Esta sección solo se aplica a los módulos de almacenamiento de controladora dual.

NOTA: También puede configurar y supervisar los sled de almacenamiento mediante la Administración integrada completa (CEM) de iDRAC. Para obtener más información, consulte la *Guía de usuario de Integrated Dell Remote Access Controller (iDRAC)*.

Temas:

Configuración de sleds de almacenamiento en modo único dividido

En el modo único dividido, las dos controladoras RAID se asignan a un único sled de cálculo. Ambas controladoras se activan y cada una de ellas se conecta a ocho unidades de disco.

Configuración de sleds de almacenamiento en modo dual dividido

En el modo dual dividido, ambas controladoras RAID de un sled de almacenamiento están conectadas a dos sleds de cálculo.

Si un sled de almacenamiento se ubica debajo de un sled FC830 PowerEdge de ancho completo, se puede configurar en el modo dual dividido. Pero las controladoras están conectadas a un único sled de cálculo y solo se informa dicho sled de cálculo.

Si un sled de almacenamiento está configurado en modo dual dividido y se encuentra en una ubicación donde no se puede conectar a dos sleds de cálculo, la segunda controladora no se conecta a ningún sled de cálculo.

Debe tener privilegio de **Administrador de configuración del chasis** y apagar el sled de cálculo antes de cambiar la configuración.

Configuración de sleds de almacenamiento en modo unido

En el modo unido, las controladoras RAID se asignan a un único sled de cálculo. Sin embargo, solo se activa una controladora y todas las unidades de disco se conectan a la misma.

Configuración de sleds de almacenamiento mediante la interfaz web de la CMC

1. En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del servidor** y haga clic en un sled de almacenamiento.
   Aparecerán los detalles del sled de almacenamiento.
2. En el menú ubicado en el lado derecho, haga clic en **Configuración**.
   Aparecerá la página **Configuración de almacenamiento**.

   También puede acceder a la página **Configuración de almacenamiento** al seleccionar un sled de almacenamiento en la página **Condición del chasis**. En **Vínculos rápidos**, haga clic en **Estado del arreglo de almacenamiento**.
3. En **Componentes**, seleccione una de las siguientes opciones:
   - **Host dual dividido**
   - **Host individual dividido**
   - **Unido**

   NOTA: Apague el sled de cálculo antes de configurar el sled de almacenamiento. Haga clic en **Control de alimentación del servidor** en la parte superior de la página para apagar el sled de cálculo. Para obtener más información, consulte la Ayuda en línea.
4. Haga clic en **Aplicar**.

Configuración de sleds de almacenamiento mediante RACADM

Puede conectar los sled de almacenamiento con los sled de cálculo mediante el comando RACADM `config` o `getconfig` con la opción `cfgStorageModule`. Para obtener más información, consulte la sección **getstoragemoduleinfo** en la *Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/manuals**.

Administración de sleds de almacenamiento mediante el proxy de RACADM del iDRAC

La función proxy de RACADM del iDRAC le permite administrar los sleds de almacenamiento en el chasis FX2s a través de RACADM del iDRAC cuando la CMC no está en la red.

Para acceder al iDRAC de manera local, utilice el siguiente comando:

```
racadm <command> --proxy
```

Ejemplo: `racadm getractime --proxy`

También puede acceder al RACADM de iDRAC de forma remota. Para obtener más información, consulte la sección "*Proxy de RACADM*" en la *Guía de referencia de la interfaz de línea de comandos RACADM de Integrated Dell Remote Access Controller 8 (iDRAC8) versión 2.10.10.10*.

NOTA: En esta versión solo se admiten proxis de RACADM locales y remotos.

Visualización de estado del arreglo de almacenamiento

En el panel izquierdo, haga clic en **Descripción general del chasis** > **Descripción general del servidor** > **<sled de almacenamiento>**. La página **Estado de la matriz de almacenamiento** se muestra en el panel de la derecha. También puede acceder a la página **Estado de la matriz de almacenamiento** de la página **Condición del chasis**.

1. En la página **Condición del chasis**, haga clic en un sled de almacenamiento en la imagen del panel frontal.
   Los detalles del sled de almacenamiento se muestran en la parte inferior del panel derecho.
2. En **Vínculos rápidos**, haga clic en **Estado del arreglo de almacenamiento**.

Para obtener más información, consulte la Ayuda en línea.

9

Configuración de la CMC para enviar alertas

Es posible configurar alertas y acciones para ciertos eventos que se producen en el chasis. Un suceso se produce cuando el estado de un componente del sistema es mayor que la condición definida previamente. Si un evento coincide con un filtro de eventos y usted ha configurado este filtro para que genere un mensaje de alerta (alerta por correo electrónico o captura de SNMP), entonces se envía una alerta a uno o varios de los destinos configurados, como dirección de correo electrónico, dirección IP o un 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 de la 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**.

Activación o desactivación de alertas mediante RACADM

Para activar o desactivar la generación de alertas, utilice el objeto RACADM `cfgAlertingEnable`. Para obtener más información, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

Filtrado de alertas

Es posible filtrar las alertas por categoría y gravedad.

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.

NOTA: Para obtener más información sobre el protocolo de configuración de SNMP y el formato de captura, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

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 árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Alertas** > **Configuración de capturas**. Aparecerá la página **Destino de alertas de sucesos del chasis**.
2. Introduzca lo siguiente:
   - En el campo **Destino**, introduzca 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` o `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 una cadena de comunidad válida a la que pertenezca la estación de administración de destino.

     Esta cadena de comunidad es distinta de la que se muestra en la página **Chasis** > **Red** > **Servicios**. La cadena de comunidad de capturas SNMP es la comunidad que la CMC utiliza para las capturas salientes destinadas a las estaciones de administración. La cadena de comunidad de la página **Chasis** > **Red** > **Servicios** es la cadena de comunidad que las estaciones de administración utilizan para consultar el daemon SNMP en la CMC.

     NOTA: El CMC utiliza una cadena de comunidad SNMP predeterminada como opción pública. Para garantizar mayor seguridad, se recomienda cambiar la cadena de comunidad predeterminada y establecer un valor que no sea uno en blanco.
   - En **Activada**, seleccione la casilla 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: Sólo se puede seleccionar una máscara de filtro para las alertas tanto de SNMP como por correo electrónico. Puede ignorar el paso 2 si ya ha seleccionado la máscara de filtro.
2. Active la generación de alertas:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
3. Active las alertas de capturas:

   ```
   racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
   ```

donde <index> es un valor entre 1 y 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 plenamente calificados (FQDN).

4. 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.

5. 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.

NOTA: El CMC utiliza una cadena de comunidad SNMP predeterminada como opción pública. Para garantizar mayor seguridad, se recomienda cambiar la cadena de comunidad predeterminada y establecer un valor que no sea uno en blanco.

Se pueden configurar hasta cuatro destinos para recibir alertas de capturas. Para agregar más destinos, repita los pasos 2 a 5.

NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice que se ha 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` .

6. 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 sabe con seguridad cuál es el número de índice, use:

```
racadm getconfig -g cfgTraps -i <index>
```

Configuración de los valores de alerta por correo electrónico

Cuando la CMC detecta un suceso del chasis, como una advertencia del entorno o una falla en un componente, se puede configurar para enviar una alerta por correo electrónico a una o más direcciones de correo electrónico.

Es necesario configurar 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 en 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 la CMC está configurado para que el servidor de correo reciba alertas por correo electrónico desde la CMC.

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 de la CMC

Para configurar los valores de alerta por correo electrónico mediante la interfaz web:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **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 las alertas. Para obtener información acerca de los campos, consulte *Ayuda en línea para la CMC*.

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 de 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
```

3. Active la generación de alertas por correo electrónico:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
```

donde `<index>` es un valor de entre 1 y 4. La CMC utiliza el número de índice para distinguir hasta cuatro direcciones de correo electrónico de destinos configurables.

4. 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.

5. 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.

6. 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, repita los pasos 2 a 5.

NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice que ha especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba:x `.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 de la línea de comandos RACADM para el iDRAC y el CMC* disponible en **dell.com/support/manuals**.

10

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 mantener la seguridad del sistema. De manera predeterminada, la CMC está configurada con una cuenta raíz predeterminada. 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 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 máximos privilegios 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 en el caso de que un usuario de la CMC tenga privilegios de **Administrador del servidor**, los privilegios otorgados al usuario de la CMC no se transferirán automáticamente al mismo usuario en un servidor, ya que los usuarios del servidor se crean independientemente de los usuarios de CMC. En otras palabras, los usuarios de Active Directory de CMC y los usuarios de Active Directory de 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 no pueden crear un usuario del servidor desde CMC ni viceversa. Esta regla protege la seguridad e integridad de los servidores.

Tabla 17. 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 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.

Tabla 17. Tipos de usuarios (continuación)

Privilegio	Descripción
	• 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 de los propios servidores. Por este motivo, los nombres y las prioridades de las ranuras se pueden agregar o cambiar sin importar si los servidores están presentes en las ranuras o no. • Está asociado con Active Directory (AD), como la administración del certificado de AD y la configuración de grupos, dominios y privilegios de AD. 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 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 del **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 del **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 del **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. Si el usuario existe en el servidor de destino y la contraseña coincide, el servidor responderá según los privilegios que el usuario tenga en el servidor. En función de los privilegios que respondan del 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:

Tabla 17. Tipos de usuarios (continuación)

Privilegio	Descripción
	• 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.

Los grupos de usuarios de la 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 18. 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 • 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)

Tabla 18. Privilegios del grupo de la CMC (continuación)

Grupo de usuarios	Privilegios otorgados
	• Administrador del servidor • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A
Ninguno	Sin permisos asignados

Tabla 19. 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 de la CMC, verifique 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 modificar a través de 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 de la 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: La ID de usuario 1 es la cuenta de usuario raíz que se envía de forma predeterminada con una CMC. Este valor no se puede modificar.

3. Active la ID de usuario y especifique el nombre de usuario, la contraseña y los privilegios de acceso para el usuario. Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea*.
4. Haga clic en **Aplicar**. El usuario se crea con los privilegios adecuados.

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 CMC o ha utilizado el comando `racresetcfg` de racadm, la única cuenta de usuario actual es la cuenta root predeterminada. 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 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 `config` de racadm, 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 config -f racadm.cfg` de racadm para especificar cualquier número de grupos u objetos para escritura, el índice no se puede especificar. Se agrega un usuario nuevo 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.

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 autentificación 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 flexibilidad máxima a la hora de configurar el acceso de usuario en distintos 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, un objeto de grupo estándar se utiliza como grupo de funciones. Un usuario con acceso a la CMC es miembro del grupo de funciones. Para conceder a este usuario acceso a una tarjeta CMC específica, el nombre del grupo de funciones y su nombre de dominio deben configurarse en la tarjeta CMC específica. 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 enumera los privilegios predeterminados del grupo de funciones.

Tabla 20. : 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.

Descripción general del esquema extendido de Active Directory

El uso del esquema extendido requiere la extensión del esquema de Active Directory.

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.

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 la 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 continúan almacenándose en la CMC para la autorización, de forma similar a la configuración del Esquema estándar compatible con Active Directory.

Para habilitar al usuario LDAP para acceder a una tarjeta CMC específica, el nombre del grupo de funciones y su nombre de dominio deben configurarse en la tarjeta CMC específica. Puede configurar hasta cinco grupos de funciones en cada CMC. Un usuario cuenta con la opción de ser agregado a varios grupos dentro del servicio de directorio. Si un usuario es miembro de varios grupos, el usuario obtiene los privilegios de todos sus grupos.

Configuración del directorio LDAP genérico para acceder a la 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.

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web de la 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.
   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 de vinculación.

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`.

Los inicios de sesión de LDAP se pueden configurar de varias maneras. En la mayoría de los casos, algunas opciones pueden utilizarse con su configuración predeterminada.

NOTA: Se recomienda seriamente utilizar el comando `testfeature -f LDAP` de racadm 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 la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/manuals**.

11

Configuración de la 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 autentificación, otorgando acceso a los usuarios que hayan iniciado sesión de manera única o automática a aplicaciones posteriores 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 otras 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 últimas revisiones y paquetes de servicio instalados en el sistema cliente. Si usa Active Directory en Microsoft Windows 2008, asegúrese de tener instalado SP1 junto con las siguientes correcciones urgentes:

  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= 32 BC1BEEA3F9-4C13-9C99-220B62A191EE&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 dominio 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** 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, cree una cuenta de usuario de Active Directory para su uso con la opción **-mapuser** del comando `ktpass`. Use el mismo nombre que el nombre DNS de la CMC en el que carga 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 siguiente comando `ktpass` para crear el archivo keytab de Kerberos:

```
C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM - mapuser dracname -mapOp
set -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

NOTA: `cmcname.domainname.com` debe estar en minúsculas, de conformidad con RFC, y `@REALM_NAME` debe estar en mayúsculas. Además, la CMC admite los tipos de criptografía DES-CBC-MD5 y AES256-SHA1 para la autentificación 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 de la 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 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 **Avanzada**.
5. En la sección **Excepciones**, agregue las direcciones para las CMC e iDRAC de la red de administración a la lista separada por punto y coma. Es posible usar nombres DNS y comodines en las anotaciones.

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 para**, 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.

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 la 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`

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 información acerca de las opciones, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.

1. Durante la configuración de 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.

   La ejecución correcta de un comando indica que la CMC puede adquirir credenciales de Kerberos y acceder a la cuenta de Active Directory del usuario. Si el comando no se ejecuta correctamente, resuelva el error y vuelva a ejecutar el comando. Para obtener más información, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* 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. 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 la 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`

12

Configuración de la 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 de la CMC (o la consola en serie/Telnet/Secure Shell) y se explica cómo configurar el sistema para que pueda realizar acciones de administración del sistema 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 la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

Temas:

Funciones de la consola de línea de comandos de la 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 de 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 de la CMC

Al conectarse a la línea de comandos de la CMC, puede ingresar estos comandos:

Tabla 21. Comandos para la interfaz de la línea de comandos de la CMC

Comando	Descripción
`racadm`	Los comandos RACADM comienzan con la palabra clave `racadm` y, a continuación, están seguidos por un subcomando. Para obtener más información, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.
`connect`	Se conecta a la consola en serie de un servidor o módulo de I/O. Para obtener más información, consulte Conexión a servidores o módulos de I/O con el comando Connect. **NOTA:** También puede usar el comando RACADM `connect`.
`exit`, `logout` y `quit`	Todos los comandos ejecutan la misma acción. Finalizan la sesión actual y regresan a una interfaz de línea de comandos de inicio de sesión.

Uso de una consola Telnet con la 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 una 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 la revisión 824810 en **support.microsoft.com**. Para obtener más información, también puede consultar el artículo 824810 de Microsoft Knowledge Base.

Uso de SSH con la 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 mayor 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 no es controlado por la CMC. Revise los mensajes de RACLog para determinar la causa de la falla.

NOTA: `OpenSSH` se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. También puede ejecutar `OpenSSH` mediante `Putty.exe`. Al ejecutar `OpenSSH` ante la petición de comandos de Windows, no se obtendrá funcionalidad completa (es decir, algunas teclas no responden y no se muestran gráficos). En los servidores que ejecutan Linux, ejecute los servicios del cliente de SSH para conectarse a la CMC con cualquier shell.

Se admiten cuatro sesiones simultáneas de SSH por vez. El tiempo de espera de la sesión es controlado por la propiedad. `cfgSsnMgtSshIdleTimeout` Para obtener más información acerca de los comandos RACADM, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* disponible en dell.com/support/Manuals.

La CMC también admite la autentificación de clave pública (PKA) por SSH. Este método de autentificación mejora la automatización de las secuencias de comandos de SSH al evitar la necesidad de incorporar o solicitar ID/contraseña de usuario.

La opción SSH está activada de manera predeterminada. Cuando la opción SSH está desactivada, es posible activarla por medio de cualquier otra interfaz admitida.

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 22. 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

Tabla 22. Esquemas de criptografía (continuación)

Tipo de esquema	Esquema
	• 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 pueden utilizarse con el nombre de usuario del servicio en una interfaz de SSH. Antes de agregar o eliminar claves públicas, asegúrese de usar el comando `view` para ver las claves que ya están configuradas, de modo que una clave no se sobrescriba ni se elimine accidentalmente. El nombre de usuario del servicio es una cuenta de usuario especial que se puede utilizar cuando se accede a la CMC a través de SSH. Cuando se configura y se utiliza correctamente la PKA en SSH, no es necesario ingresar un nombre de usuario ni una contraseña para iniciar sesión en la CMC. Esto puede ser muy útil para configurar scripts automatizados con el fin de ejecutar diversas funciones.

NOTA: No hay soporte de interfaz gráfica de usuario para administrar esta función; solamente se puede utilizar RACADM.

Cuando se agregan claves públicas nuevas, asegúrese de que las claves existentes no se encuentren en el índice, donde se agrega la clave nueva. La CMC no realiza comprobaciones para asegurarse de que las claves anteriores se eliminen antes de agregar una nueva. Ni bien se agrega una clave nueva, esta entra en vigor automáticamente, siempre y cuando la interfaz de SSH esté activada.

Cuando utilice la sección comentario de clave pública de la clave pública, recuerde que la CMC utiliza solo los primeros 16 caracteres. La CMC utiliza el comentario de clave pública para distinguir a los usuarios SSH cuando usan el comando RACADM `getssninfo`, ya que todos los usuarios de PKA utilizan el nombre de usuario del 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 la *Guía de referencia de la línea de comandos de Chassis Management Controller para PowerEdge FX2/FX2s*.

Configuración del software de emulación de terminal

La CMC admite una consola de texto de serie que se puede iniciar mediante cualquier software de emulación de terminal. A continuación, se incluyen algunos ejemplos de este tipo de software que se puede utilizar para conectarse a la CMC.

1. Minicom de Linux
2. HyperTerminal de Hilgraveve para Windows

Conecte un extremo del cable de módem nulo serie (presente en ambos extremos) al conector serie en la parte posterior del chasis. Conecte el otro extremo del cable al puerto de serie de la estación de administración. Para obtener más información sobre la conexión de cables, consulte el panel posterior del chasis en la sección Descripción general del chasis.

Configure su software de emulación de terminal con los siguientes parámetros:

- **Velocidad en baudios**: 115200
- **Puerto**: COM1
- **Datos**: 8 bits
- **Paridad**: ninguna
- **Detener**: 1 bit
- **Control de flujo de hardware**: Sí
- **Control de flujo de softwarel**: No

Conexión a servidores o módulos de I/O 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 ejecutar los comandos RACADM, consulte la *Guía de referencia sobre línea de comandos RACADM de Chassis Management Controller para PowerEdge FX2/FX2s*.
- 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 en serie, Telnet, SSH, la CMC admite el comando `connect` para establecer una conexión en serie a un servidor o un módulo de I/O. La consola en serie del servidor contiene las pantallas de inicio y configuración del BIOS y la consola en serie del sistema operativo. Para el módulo de I/O, está disponible la consola en serie del switch. Hay un solo módulo de I/O en el chasis.

PRECAUCIÓN: Cuando se ejecuta desde la consola en serie de la CMC, la opción `connect -b` permanece conectada hasta que se restablece la CMC. Esto supone un posible riesgo de seguridad.

NOTA: El comando `connect` proporciona la opción `-b` (binario). La opción `-b` pasa datos binarios sin procesar y no se usa `cfgSerialConsoleQuitKey`. Además, cuando se conecta a un servidor mediante la consola en serie de la CMC, las transiciones en la señal DTR (por ejemplo, si se quita el cable en serie para conectar un depurador) no provocarán que salga de la aplicación.

NOTA: Si el módulo de I/O no admite la redirección de consola, el comando `connect` muestra una consola vacía. En ese caso, para regresar a la consola de la CMC, escriba la secuencia de escape. La secuencia de escape predeterminada de la consola es <Ctrl><\>.

Para conectarse a un módulo de E/S escriba:

```
connect switch-n
```

en donde `n` es un módulo de I/O 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 23. Asignación de módulos de E/S en conmutadores

Etiqueta del módulo de E/S	Conmutador
A1	switch-a1 o switch- 1
A2	conmutador-a2 o conmutador- 2

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 en serie de servidor administrado, ejecute el comando `connect server-n` , donde *n* = 1-4 (PowerEdge FM120x4) y *n* = 1-8 (PowerEdge FC630). También puede utilizar el comando `racadm connect server-n`. Cuando se conecta a un servidor con la opción `-b`, se supone que existe una comunicación binaria y el carácter de escape está deshabilitado. Si el iDRAC no está disponible, se mostrará el mensaje de error `No route to host`.

El comando `connect server-n` permite que el usuario acceda al puerto serial del servidor. Una vez establecida la conexión, el usuario puede ver la redirección de consola del servidor a través del puerto serial de la CMC que incluye la consola en serie del BIOS y la consola en serie del sistema operativo.

NOTA: Para ver las pantallas de inicio del BIOS, se debe activar la redirección en serie en la configuración del BIOS de los servidores. Además, debe establecer la ventana del emulador de terminal en 80 × 25. De lo contrario, los caracteres en la página no se mostrarán de forma correcta.

NOTA: Todas las claves no funcionan en las páginas de configuración del BIOS. Por lo tanto, proporcione los accesos directos de teclado adecuados para <Ctrl> <Alt> <Delete> y otros. La pantalla de redirección inicial muestra los accesos directos de teclado necesarios.

Configuración del BIOS del servidor administrado para la redirección de consola serie

Puede usar una sesión de consola remota para conectarse con el sistema administrado mediante la interfaz web de iDRAC7 (consulte la *Guía del usuario de Dell Integrated Dell Remote Access Controller (iDRAC)*, en **dell.com/support/manuals**.

De forma predeterminada, se apaga la comunicación en serie en el BIOS. Para redirigir los datos de la consola de texto del host a la comunicación en serie en la LAN, debe activar la redirección de 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 <Intro>. 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 del inicio** (el valor predeterminado está **desactivado**). Esta opción activa la redirección de consola del BIOS en los reinicios subsiguientes.
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 recibe información del BIOS y activa la Consola de administración especial (SAC), consola uno COM1.

Configuración de Linux para la redirección de la consola en serie del servidor durante el inicio

Los pasos siguientes son específicos para 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`, coméntela.

   El siguiente ejemplo ilustra los cambios descritos en este procedimiento.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making
changes
# to this file
```

```
# NOTICE: You do not have a /boot partition. This
means that
# all kernel and initrd paths are relative to
/, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=
/dev/sdal
# initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial
title Red Hat Linux Advanced Server (2.4.9-e.3smp)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=
/dev/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 carácter de comentario al inicio de la línea 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 agregado `console=ttyS1,57600` 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
```

Administración de la CMC mediante el proxy de RACADM del iDRAC

La CMC se puede administrar mediante el proxy de RACADM del iDRAC cuando la CMC no está en la red. La siguiente tabla indica la asignación de privilegios de la CMC con privilegios del iDRAC para la operación de proxy.

Tabla 24. Asignación de los privilegios de la CMC e iDRAC

Privilegio de la CMC	Se necesita privilegio de iDRAC para la operación de proxy
Usuario con acceso a la CMC	Inicio de sesión del iDRAC
Administrador de configuración del chasis	Configurar iDRAC
Administrador de configuración de usuarios	Configurar usuarios en el iDRAC
Administrador de borrado de registros	Registros
Administrador de control del chasis	Control del sistema
Administrador del servidor	Control del sistema
Usuario de alertas de prueba	Operaciones del sistema
Administrador de comandos de depuración	Depuración
Administrador de red Fabric x (donde x es A, B o C)	Control del sistema

Para obtener más información, consulte la *Dell Chassis Management Controller Version 2.0 for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller versión 1.2 para PowerEdge FX2/FX2s).

13

Uso de las tarjetas FlexAddress y FlexAddress Plus

Esta sección proporciona información acerca de FlexAddress y cómo utilizar FlexAddress Plus para configurar la función FlexAddress.

NOTA: La función FlexAdress está bajo licencia. Esta licencia de función se incluye en la licencia Enterprise.

Temas:

Acerca de FlexAddress

FlexAddress permite que la CMC asigne ID de WWN/MAC a una ranura determinada y sobrescriba las ID de fábrica. Por lo tanto, si se sustituye el módulo del servidor, la ID de WWN/MAC basada en la ranura no se modifica. Gracias a esta función, ya no es necesario volver a configurar las herramientas de administración de red Ethernet, los recursos SAN, los servidores DHCP y los enrutadores de diferentes redes Fabric para un nuevo módulo de servidor.

A cada módulo del servidor se le asignan ID WWN y/o MAC exclusivas como parte del proceso de fabricación. Antes de FlexAddress, si se tenía que reemplazar el módulo de un servidor por otro, las ID WWN/MAC se cambiaban, y las herramientas de administración de red Ethernet y los recursos SAN debían configurarse nuevamente para identificar el nuevo módulo del servidor.

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 tenga la función FlexAddress activada para la ranura nueva. De ser desmontado el servidor, regresará a la dirección asignada por el servidor.

Además, la acción *sustitución* 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 ID de WWN/MAC asignadas de fábrica.

El chasis FX2/FX2S de la CMC se envía con la Tarjeta SD FlexAddress Plus, que admite las funciones FlexAddress, FlexAddress Plus y Almacenamiento extendido.

NOTA: La información contenida en la tarjeta SD FlexAddress Plus está cifrada y no es posible duplicarla o alterarla de ninguna manera porque podría desactivar las funciones del sistema y hacer que deje de funcionar correctamente.

NOTA: El uso de una tarjeta SD FlexAddress Plus se limita a un solo chasis. No puede usar la mista tarjeta SD FlexAddress Plus en otro chasis.

Acerca de FlexAddress Plus

Cada tarjeta de función FlexAddress Plus contiene agrupación única de MAC/WWN que le permiten al chasis asignar 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 global y específicas para una ranura del servidor.

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 vacío en la tarjeta SD contiene una etiqueta XML `mac_start` que es la primera dirección MAC hexadecimal de inicio que se usa para este rango

exclusivo de direcciones MAC. La etiqueta `mac_count` es el número total de direcciones MAC que asigna la tarjeta SD. Para determinar el rango total de MAC asignado, use la siguiente fórmula:

```
<mac_start> + <mac_count> - 1 = <mac_end>
```

Por ejemplo:

```
(starting_mac)00:18:8B:FF:DC:FA + (mac_count)0xCF – 1 = (ending_mac)00:18:8B:FF:DD:C8
```

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.

Verificación de la activación de FlexAddress

Para ver el estado de activación de la función FlexAddress, ejecute el siguiente comando RACADM:

```
racadm featurecard -s
```

```
        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
```

If there are no active features on the chassis, the command returns a message: racadm feature -s No features active on the chassis

```
racadm feature -s
No features active on the chassis
```

Para ver la información de la tarjeta SD:

```
$ racadm featurecard -s
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
```

Tabla 25. 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.
`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.

Tabla 25. Mensajes de estado que muestra el comando featurecard -s (continuación)

Mensaje de estado	Acciones
`The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.`	La tarjeta de función se puede mover a otro chasis o se puede reactivar en el chasis actual. Para reactivar en el chasis actual, introduzca `racadm racreset` hasta que se active el módulo de CMC con la tarjeta de función instalada.

Las tarjetas de funciones de Dell pueden contener más de una función. Una vez que se haya activado en un chasis cualquier función incluida en una tarjeta de función de Dell, cualquier otra función que pueda incluirse en esa tarjeta de función de Dell no podrá activarse en otro chasis. En este caso, el comando -s de la función RACADM 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 sobre los comandos `feature` y `featurecard`, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

Desactivación de FlexAddress

Es posible desactivar la función FlexAddress y hacer que la tarjeta SD regrese a un estado previo a la instalación mediante un comando de RACADM. No hay ninguna función de desactivación en la interfaz web. La desactivación hace que la tarjeta SD regrese a su estado original, donde se la puede instalar y activar en otro chasis. En este contexto, el término FlexAddress implica tanto FlexAddress como FlexAddressPlus.

NOTA: La tarjeta SD debe estar instalada físicamente en el CMC y el chasis debe estar apagado antes de ejecutar el comando de desactivación.

Si ejecuta el comando de desactivación sin instalar una tarjeta SD o con una tarjeta desde un chasis diferente instalado, la función se desactiva y no se realiza el cambio en la tarjeta.

Para desactivar la función FlexAddress y restablecer la tarjeta SD:

```
racadm feature -d -c flexaddress
```

El comando muestra el siguiente mensaje de estado si se desactivó correctamente.

```
feature FlexAddress is deactivated on the chassis successfully.
```

Si el chasis no se apaga antes de ejecutar el comando, el comando muestra el siguiente error:

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

NOTA: Para activar la función FlexAddress de nuevo, vuelva a iniciar el CMC.

Para obtener más información acerca del comando, consulte la sección del comando **feature** de la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

Configuración de FlexAddress

FlexAddress es una actualización opcional que permite a los módulos de los servidores reemplazar la identificación WWN/MAC asignada de fábrica por una identificación WWN/MAC proporcionada por el chasis.

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 *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/cmcmanuals**.

El servidor debe estar apagado antes de 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 las ranuras que activará. 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: Cuando se implementa la función FlexAddress por primera vez en un módulo de servidor determinado, 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, para lo que se debe encender el módulo del servidor. Cuando se completan las secuencias de apagado y encendido, las ID MAC asignadas por el chasis están 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 luego, se seleccionan las ranuras que deben participar en la función. Tanto las redes Fabric como las ranuras deben activarse para configurar FlexAddress satisfactoriamente.

Visualización del Nombre mundial o las ID de control de acceso a medios ID.

La página **Resumen de WWN/MAC** permite ver la configuración del Nombre mundial (WWN) y la dirección de Control de acceso a medios (MAC) de una ranura en el chasis.

Mensajes de comandos

En la siguiente tabla se muestran los comandos RACADM y los mensajes de situaciones comunes de FlexAddress.

Tabla 26. Comandos y salida de FlexAddress

Situación	Comando	Salida
La tarjeta SD en el módulo de la CMC activo está vinculada a otra etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`
La tarjeta SD en el módulo de la CMC activo está vinculada a la misma etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound`
La tarjeta SD en el módulo de la CMC activo no está vinculada a ninguna etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress:not bound`
La función FlexAddress no está activada en el chasis por algún motivo (no hay tarjeta SD insertada, tarjeta SD dañada, después de haber desactivado la función, tarjeta SD vinculada a otro chasis).	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotstate>]`	`ERROR: Flexaddress feature is not active on the chassis`

Tabla 26. Comandos y salida de FlexAddress (continuación)

Situación	Comando	Salida
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.` **NOTA:** Para solucionar este problema, debe contar con una licencia de **Activación de FlexAddress**.

CONTRATO DE LICENCIA DE SOFTWARE DE DELL FlexAddress

El presente 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 de Dell, para el cual 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 propietario del Software. Todos los derechos no otorgados expresamente en virtud de este contrato son reservados por el fabricante o propietario del Software. Al abrir o romper el sello del o los paquetes de Software, instalar o descargar el Software, o utilizar el Software cargado previamente o incluido en el producto, usted acepta estar sujeto a los términos de este contrato. Si no acepta estos términos, devuelva de inmediato todos los artículos de Software (discos, material escrito y embalaje) y elimine todo Software cargado previamente o incluido.

Puede utilizar una copia del Software únicamente en un equipo a la vez. Si dispone de varias licencias de Software, podrá utilizar tantas copias a la vez como licencias tenga. Por "utilizar" se entiende cargar el Software en la memoria temporal o en el almacenamiento permanente del equipo. Su instalación en un servidor de red únicamente con motivo de distribución a otros equipos no implica "utilizar" si (pero solo si) usted dispone de una licencia por separado para cada equipo al que se haya distribuido el Software. Debe asegurarse de que la cantidad de personas que utilizan el Software instalado en un servidor de red no es superior al número de licencias de las que dispone. Si la cantidad 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 coincida con 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 sobre el uso que usted hace del Software durante el horario laboral normal, acepta cooperar con Dell en dicha auditoría y acepta proporcionar a Dell todos los informes relacionados razonablemente con el uso que usted hace del Software. La auditoría queda sujeta 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 hacer una sola copia del Software únicamente con motivos de archivado o copia de respaldo, o transferirlo a un único disco duro siempre que conserve el original con motivos de archivado o copia de respaldo. No puede alquilar o arrendar el Software 240 Uso de las tarjetas FlexAddress y FlexAddress Plus ni copiar el material impreso que se incluye con el Software, pero sí puede transferir el Software, junto con todos material adjunto de manera permanente como parte de la venta o transferencia del producto de Dell, siempre y cuando no conserve 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 ingeniería inversa, descompilar o desensamblar el Software. Si el paquete que viene con su equipo contiene discos compactos, disquetes 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 de material o 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 limitará a (a) la devolución del importe abonado por el Software o (b) la sustitución de los discos que no cumplan con esta garantía y que usted envíe a Dell con un número de autorización de devolución, por su cuenta y riesgo. Esta garantía limitada quedará sin efecto 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 durante treinta (30) días, conforme lo que resulte mayor.

Dell NO garantiza que las funciones del Software estarán a la altura de 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 EL DE SUS PROVEEDORES, RENUNCIA A CUALQUIER OTRA GARANTÍA, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, SIN LÍMITE, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN PROPÓSITO DETERMINADO, EN LO QUE RESPECTA AL SOFTWARE Y A TODOS LOS MATERIALES ESCRITOS QUE LO ACOMPAÑAN. Esta garantía limitada le otorga derechos legales específicos, aunque puede 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 LÍMITE, LOS DAÑOS POR PÉRDIDA DE BENEFICIOS, 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 SE ENCUENTRA", SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA; INCLUIDA, SIN LÍMITE, LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O IDONEIDAD PARA UN FIN ESPECÍFICO. EN NINGÚN CASO DELL, LOS PROPIETARIOS DE LOS DERECHOS DE AUTOR O COLABORADORES SERÁN RESPONSABLES POR NINGÚN DAÑO DIRECTO, INDIRECTO, INHERENTE, ESPECIAL, EJEMPLAR O CONSIGUIENTE (LO QUE INCLUYE, SIN LÍMITE, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTOS, LA PÉRDIDA DE USO, DATOS O GANANCIAS; O LA INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL), CUALQUIERA QUE 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, y están compuestos por "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. 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 el presente.

El contratante/fabricante es Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

GENERAL

Esta licencia estará en vigor hasta que finalice. Dicha finalización se producirá en virtud de las condiciones estipuladas anteriormente o si usted no cumple con alguno de estos términos. Al finalizar, usted acepta que procederá a la destrucción del Software y de los materiales que lo acompañan, así como de todas sus copias. Este contrato se rige 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, los términos o las condiciones de este contrato. Este contrato es vinculante para los sucesores y cesionarios. Tanto Dell como usted aceptan renunciar, conforme lo permitido por la ley, a cualquier derecho a un proceso con jurado con respecto al Software o este contrato. Como esta renuncia de derechos puede no ser efectiva en ciertas jurisdicciones, es posible que no se aplique en su caso. Usted reconoce que ha leído el presente contrato, que lo entiende y acepta estar sujeto a sus términos, y que esta es la declaración completa y exclusiva del contrato entre usted y Dell con respecto al Software.

Visualización de la información de direcciones 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 del iDRAC se considera parte de la red Fabric de administración y se muestra junto con el resto de las redes Fabric.
  - Una marca de verificación verde indica que la red Fabric está activada para FlexAddress o FlexAddressPlus.

- Protocolo que se utiliza en el puerto del Adaptador NIC. Por ejemplo, LAN, iSCSI, FCoE, y así sucesivamente.
- 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 actual: asignado por el servidor, FlexAddress o MAC de la identidad de E/S. Una marca verde indica el tipo de dirección activada, 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. En base a 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 las direcciones WWN/MAC para ranuras específicas mediante la página **FlexAddress** (haga clic en **Descripción general del servidor** > **Ranura <x>** > **Configuración** > **FlexAddress**). Puede ver la información de las direcciones WWN/MAC para todas las ranuras y el servidor a través de la página **Resumen WWN/MAC** (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 la ranura del servidor, la red Fabric, el protocolo, las direcciones WWN/MAC y el estado de la partición. Solo las direcciones MAC activas se muestran en el campo 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 de una ranura o haga clic en **Expandir/Contraer todo** 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 sobre los campos, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.

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 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.
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 todas las MAC o las MAC asociadas con el protocolo seleccionado.
8. En el campo **Direcciones WWN/MAC**, para filtrar una ranura asociada con la dirección MAC específica, introduzca la dirección MAC exacta. De manera alternativa, introduzca parcialmente las anotaciones de la dirección MAC para ver las ranuras asociadas. Por ejemplo, ingrese `4A` para ver las ranuras con direcciones MAC que contengan `4A`.
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, la fila que muestra la partición aparece atenuada.

Para obtener información sobre los campos, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.

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 pueden ver la Ranura del servidor, la red Fabric, el Protocolo, las Direcciones WWN/MAC, el tipo de asignación de direcciones MAC (asignada por el servidor, FlexAddress o MAC de identidad de E/S) y el Estado de la partición. Una marca verde indica el tipo de dirección activada, ya sea asignada por el servidor, por el chasis o de manera remota. MAC. Si un servidor no tiene la función de FlexAddress o Identidad de E/S activada, el estado **FlexAddress (asignada por el chasis)** o **Identidad de E/S (asignada en forma remota)** se muestra como **No activado**.
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. De manera alternativa, introduzca parcialmente las anotaciones de la dirección MAC para ver las ranuras asociadas. Por ejemplo, ingrese `4A` para ver las ranuras con direcciones MAC que contengan `4A`.
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 sobre los campos, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.

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 las direcciones MAC iSCI de Ethernet de todos los LOM o las tarjetas mezzanine, utilice el siguiente comando RACADM:

```
racadm getmacaddress -a
```

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 obtener más información acerca de los subcomandos `getflexaddr` y `getmacaddress`, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

14

Administración de redes Fabric

El chasis admite dos tipos de red Fabric: Fabric A1 y Fabric A2, que utilizan los dos módulos de E/S y siempre están conectados a los adaptadores Ethernet integrados de los servidores.

NOTA: En el chasis de PowerEdge FX2s, las redes Fabric B y C son la conexión de PCIe con las tarjetas de extensión de PCIe.

A continuación, se indican los módulos de E/S compatibles:

- 1GbE de paso
- 10GbE de paso
- Agregador de E/S

Las dos redes Fabric sólo admiten Ethernet. Cada adaptador de E/S del servidor (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).

NOTA: En la CLI del CMC, al módulo de E/S se lo conoce por la convención "conmutador".

Temas:

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 conmutadores 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 da lugar a 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 de la CMC

Para configurar los valores de red para los módulos de E/S:

1. En el panel izquierdo, haga clic en **Visión general del chasis**, haga clic en **Visión general del módulo de I/O** y, a continuación, haga clic en **Configuración**. Como alternativa, para configurar los ajustes de red de los módulos de I/O disponibles (**A1** y **A2**), haga clic en **Gigabit Ethernet A1** o **Gigabit Ethernet A2** 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 se permite, escriba la contraseña raíz, la cadena de comunidad SNMP de solo lectura y la dirección IP del servidor de registro del sistema para el módulo de I/O. Para obtener más información sobre las descripciones de los campos, consulte la *Ayuda en línea*.

   NOTA: La dirección IP configurada en el módulo de I/O desde la CMC no se guarda en la configuración de inicio permanente del switch. Para guardar la configuración de la dirección IP de forma permanente, debe ejecutar el comando `connect switch` o el comando RACADM `racadm connect switch`, o bien use una interfaz directa a la GUI del módulo de I/O 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 ajustes de red para un módulo de I/O mediante RACADM, configure la fecha y la hora. Consulte la sección del comando deploy en la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

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>
```

Visualización del estado del enlace ascendente y del enlace descendente del módulo de Entrada/Salida mediante la interfaz web

NOTA: Esta función está disponible solamente en PowerEdge FX2/FX2s.

Puede ver la información de estado del enlace ascendente y descendente del Agregador del módulo de E/S Dell PowerEdge con la interfaz web de la CMC. Para hacerlo:

1. Vaya a **Descripción general del chasis** > **Descripción general del módulo de E/S**.
   Aparecerán todos los módulos de E/S (1–2) en la lista expandida.
2. Haga clic en el módulo de E/S (ranura) que desea ver S

   Aparecerá la página de estado del módulo de E/S específica de la ranura del módulo de E/S. Aparecerán las tablas Estado del enlace ascendente del módulo de E/S y Estado del enlace descendente del módulo de E/S. Estas tablas muestran información sobre los

puertos de enlace descendente (1-8) y los puertos de enlace ascendente (9-12). Para obtener más información, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

Visualización de la información de la sesión de FCoE del módulo de Entrada/Salida mediante la interfaz web

Puede ver la información de la sesión de FCoE del agregador del módulo de E/S Dell PowerEdge con la interfaz web de la CMC. Para hacerlo:

1. Vaya a **Descripción general del chasis** > **Descripción general del módulo de E/S**.
   Aparecerán todos los módulos de E/S (2) en la lista expandida.
2. Haga clic en el módulo de E/S (ranura) que desea ver S Haga clic en **Propiedades** > **FCoE**.
   Aparecerá la página **Módulo de E/S de FCoE** específica de la ranura del módulo de E/S.
3. En el menú desplegable **Seleccionar puerto**, seleccione el número de puerto requerido para el módulo de E/S seleccionado y haga clic en **Mostrar sesiones**. La opción seleccionada recupera la información de la sesión de FCoE para el conmutador y la presenta al usuario en forma de tabla.
   La sección **Información de la sesión de FCoE** mostrará la información de la sesión de FCoE del conmutador.
   NOTA: El Agregador de E/S también mostrará las sesiones de FCoE activas cuando el conmutador esté usando el protocolo.

Restablecimiento de los módulos de E/S a la configuración predeterminada de fábrica

Puede restablecer los módulos de E/S a la configuración predeterminada de fábrica en la página **Implementar módulos de E/S**.

NOTA: Esta función solo se admite en el módulo de E/S del Agregador de E/S PowerEdge. No se admiten otros módulos de E/S, como MXL 10/40GbE.

Para restablecer los módulos de E/S seleccionados a la configuración predeterminada de fábrica mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración** o expanda **Descripción general del módulo de E/S** en el árbol del sistema, seleccione el módulo de E/S y haga clic en **Configuración**.
   La página **Implementar módulos de E/S** muestra los módulos de E/S que están encendidos.
2. En el módulo de E/S correspondiente, haga clic en **Restablecer**.
   Aparece un mensaje de aviso.
3. Haga clic en **Aceptar** para continuar.

Actualización de software del módulo de E/S mediante la interfaz web de la CMC

Para actualizar el software del módulo de E/S, seleccione la imagen de software requerida desde una ubicación especificada. También puede regresar a una versión de software anterior.

NOTA: Esta función solo se admite en el **Agregador de E/S Dell PowerEdge**.

Para actualizar el software de los dispositivos de infraestructura de módulo de E/S, en la interfaz web de la CMC:

1. Vaya a **Descripción general del chasis** > **Descripción general del módulo de E/S** > **Actualizar**.
   Se muestra la ventana Actualización del firmware del módulo de E/S. De manera alternativa, desplácese a cualquiera de las siguientes páginas:
   - **Descripción general del chasis Actualizar**.
   - **Descripción general del chasis** > **Controladora del chasis** > **Actualizar**.

   Aparece la página Actualización de firmware, que proporciona un vínculo para acceder a la página Firmware y software de módulo de E/S.
2. En la página Actualización del firmware del módulo de E/S, en la sección Firmware, seleccione la casilla de verificación en la columna Actualizar para el módulo de E/S cuyo software desea actualizar y haga clic en **Aplicar actualización de firmware**. De forma alternativa, puede regresar a versiones anteriores del software; para ello, seleccione la casilla de la columna Revertir.

3. Seleccione la imagen de software para la actualización de software utilizando la opción Explorar. El nombre de la imagen de software se visualiza en el campo Ubicación de software de módulo de E/S.
   La sección Estado de actualización proporciona información sobre el estado de la actualización o reversión de software. 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.

   NOTA: No haga clic en el icono Actualizar ni visite otra página durante la transferencia de archivos.

   NOTA: El cronómetro de transferencia de archivos no se muestra cuando se actualiza el firmware de un dispositivo de infraestructura de módulo de E/S.

   NOTA: La versión de software de FTOS o el módulo de E/S se muestra en el formato X-Y(A-B). Por ejemplo, 8-3(1-4). Si la versión de reversión de la imagen FTOS es una imagen antigua que utiliza el formato de cadena de la versión antigua 8-3-1-4, la versión actual se muestra como 8-3(1-4).

GUI de agregador de E/S o MXL

Es posible iniciar la GUI de agregador de E/S/MXL desde la CMC para administrar la configuración del agregador de E/S/MXL. Para iniciar la GUI de agregador de E/S/MXL desde la CMC, los módulos de E/S deben estar establecidos en MXL o agregador de E/S y usted debe tener privilegios de administrador de la red Fabric A.

La GUI de MXL de Dell PowerEdge FX2 admite el cambio del modo de conmutador a Agregador de E/S desde MXL y la GUI del Agregador de E/S de PowerEdge FX2 admite el cambio del modo del conmutador a MXL desde Agregador de E/S.

Puede iniciar la GUI del agregador de E/S y MXL desde las páginas **Descripción general del chasis**, **Descripción general del módulo de E/S** y **Estado del módulo de E/S**.

NOTA: Al iniciar sesión en la aplicación MXL por primera vez, se le solicitará que personalice la contraseña.

Inicio de la GUI del agregador de E/S y MXL desde la página Descripción general del chasis

Vaya a **Descripción general del chasis** > **Vínculos de acceso rápido** > **Iniciar GUI del módulo de E/S**. Se visualiza la página de inicio de sesión del agregador de E/S/MXL.

Inicio de la GUI del agregador de E/S y MXL desde la página Descripción general del módulo de E/S

En el árbol de directorios, vaya a **Descripción general del módulo de E/S**. En la página, **Estado del módulo de E/S**, haga clic en **Iniciar GUI del módulo de E/S**. Se visualiza la página de inicio de sesión del agregador de E/S/MXL.

Inicio de la GUI del agregador de E/S y MXL desde la página Estado del módulo de E/S

En el árbol de directorios, en la **Descripción general del módulo de E/S**, haga clic en un conmutador de agregador de E/S/MXL. En la página, **Estado del módulo de E/S**, haga clic en **Iniciar GUI del módulo de E/S**. Se visualiza la página de inicio de sesión del agregador de E/S/MXL.

Módulo del Agregador de Entrada/Salida

Puede consultar la información del módulo de E/S en las páginas de la interfaz de RACADM, el Estado del chasis, la Descripción general del módulo de E/S y el Estado del módulo de E/S. Esta información también se puede consultar desde el RACADM de la CMC.

Los modos de los módulos de E/S son los siguientes:

- Independiente
- Apilamiento
- PMux
- Conmutador completo

Puede ver el modo de los módulos de E/S como información sobre herramientas cuando selecciona el módulo de E/S en las páginas **Condición del chasis**, **Estado del módulo de E/S** y **Descripción general del módulo de E/S**.

Al cambiar el modo de un agregador de E/S que tiene una IP estática, de modo de apilamiento a independiente, asegúrese de que la red para el agregador se cambia en DHCP. De lo contrario, la IP estática es un duplicado en todos los agregadores de E/S.

Cuando los módulos de E/S se encuentran en modo de apilamiento, la ID de la pila es la misma que el módulo de E/S maestro grabado en la MAC durante el encendido inicial. La ID de la pila no cambia al cambiar los modos del módulo de E/S. Por ejemplo, durante el encendido inicial, si el interruptor 1 es el maestro, la dirección MAC de la pila es idéntica a la del conmutador 1 grabado en la dirección MAC. Posteriormente, cuando el interruptor 3 es el maestro, la dirección MAC del conmutador 1 se mantiene como la ID de la pila.

El comando racadm, `getmacaddress` muestra I/F MAC, que se graba en la dirección MAC + 2.

15

Uso del Administrador de VLAN

Puede asignar o ver los valores de VLAN en los módulos de E/S mediante la opción **Administrador de VLAN**.

NOTA: Esta función solo se admite en el Agregador de E/S Dell PowerEdge.

Después de que el modo del Agregador de E/S se cambia de apilamiento a independiente, extraiga la configuración de inicio y vuelva a cargar el Agregador de E/S. No es necesario guardar la configuración del sistema mientras se vuelva a cargar el Agregador de E/S.

Temas:

Asignación de VLAN a los módulos de E/S

Las LAN virtuales (VLAN) para los módulos de E/S permiten separar a los usuarios en segmentos de red individuales por motivos de seguridad y otras cuestiones. El uso de las VLAN permite aislar las redes para los usuarios individuales en un conmutador de 32 puertos. Es posible asociar los puertos seleccionados en un conmutador con VLAN seleccionadas y considerar estos puertos como un conmutador distinto.

La interfaz web del CMC permite configurar los puertos de administración en banda (VLAN) en los módulos de E/S.

Para asignar una VLAN a un módulo de E/S, vaya a **Descripción general del chasis** > **Descripción general del módulo de E/S** > **Configuración** > **Administrador de VLAN**.

En la sección **Asignación de VLAN**, seleccione el módulo de E/S y elija el tipo de configuración. Asimismo, especifique el rango de puertos y la ranura.

Cambie o edite las VLAN mediante la selección de los diferentes elementos en la lista del menú desplegable.

Configuración de los valores de VLAN en los módulos de E/S mediante la interfaz web de la CMC

Para configurar los valores de VLAN en los módulos de E/S mediante la interfaz web de la CMC:

1. Vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración administrador de VLAN**.
   La página Administrador de VLAN muestra los módulos de E/S que están encendidos y los puertos disponibles.
2. En la sección **Seleccionar módulos de E/S**, seleccione el tipo de configuración en la lista desplegable y, a continuación, seleccione los módulos de E/S requeridos.
3. En la sección **Especificar rango de puerto**, seleccione el rango de puertos de redes Fabric que desea asignar a los módulos de E/S seleccionados.
4. Seleccione la opción **Seleccionar o deseleccionar todo** para aplicar los cambios a todos o a ninguno de los módulos de E/S.

   o

   Active la casilla de las ranuras específicas para seleccionar los módulos de E/S requeridos.
5. En la sección **Editar VLAN**, introduzca las identificaciones de VLAN para los módulos de E/S. Especifique un valor entre el 1 y el 4094. Las identificaciones de VLAN se pueden introducir como un rango o separadas por coma.
6. Seleccione una de las siguientes acciones en el menú desplegable según corresponda:

- Agregar VLAN etiquetadas
- Eliminar las VAN
- Actualizar VLAN sin etiquetar
- Restablecer a todas las VLAN
- Mostrar las VLAN

7. Haga clic en **Guardar** para guardar la nueva configuración realizada en la página **Administrador de VLAN**.

   NOTA: En la sección Resumen de VLAN de todos los puertos, se puede consultar información sobre los módulos de E/S presentes en el chasis y las VLAN asignadas. Haga clic en **Guardar** para guardar un archivo csv del resumen de los valores de VLAN actuales.

   NOTA: La sección VLAN administradas del CMC muestra el resumen de todas las VLAN asignadas a los módulos de E/S.

8. Haga clic en **Aplicar**.
   Los valores de red se configuran para los módulos de E/S.

Visualización de los valores de VLAN en los módulos de E/S mediante la interfaz web de la CMC

Para ver los valores de VLAN en los módulos de E/S mediante la interfaz web de la CMC:

1. Vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración** > **Administrador de VLAN**.
   Aparecerá la página **Administrador de VLAN**. La sección Resumen de VLAN de todos los puertos muestra información sobre los valores de VLAN actuales de los módulos de E/S.
2. Haga clic en **Guardar** para almacenar los valores de VLAN en un archivo.

Visualización de la configuración actual de VLAN en los módulos de E/S mediante la interfaz web de la CMC

Para visualizar la configuración actual de VLAN en los módulos de E/S mediante la interfaz web de la CMC:

1. Vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración** > **Administrador de VLAN**.
   Aparecerá la página **Administrador de VLAN**.
2. En la sección **Editar VLAN**, seleccione **Mostrar VLAN** en la lista desplegable y haga clic en **Aplicar**.
   Se mostrará un mensaje de operación correcta. La configuración actual de las VLAN asignadas a los módulos de E/S se mostrará en el campo **Resumen de asignaciones de VLAN**.

Eliminación de las VLAN para los módulos de E/S mediante la interfaz web de la CMC

Para eliminar las VLAN desde los módulos de E/S mediante la interfaz web de la CMC:

1. Vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración** > **Administrador de VLAN.**
   Aparecerá la página Administrador de VLAN.
2. En la sección **Seleccionar módulo de E/S**, seleccione los módulos de E/S requeridos.
3. En la sección **Editar VLAN**, seleccione **Eliminar VLAN** en la lista desplegable y haga clic en **Aplicar**.
   Las VLAN asignadas a los módulos de E/S seleccionados se eliminarán.

   Se mostrará un mensaje de operación correcta. La configuración actual de las VLAN asignadas a los módulos de E/S se mostrará en el campo **Resumen de asignaciones de VLAN**.

Actualización de VLAN sin etiquetar para módulos de E/S mediante la interfaz web de la CMC

Para actualizar VLAN sin etiquetar para módulos de E/S mediante la interfaz web de la CMC:

NOTA: Las VLAN sin etiquetar no se pueden establecer en un ID de VLAN que ya está etiquetada.

1. Vaya a **Visión general del módulo de I/O** y haga clic en **Configuración** > **Administrador de VLAN**.
   Aparecerá la página Administrador de VLAN.
2. En la sección **Seleccionar módulo de E/S**, seleccione los módulos de E/S requeridos.
3. En la sección **Especificar rango de puerto**, seleccione el rango de puertos de redes Fabric que desea asignar a los módulos de E/S seleccionados.
4. Seleccione la opción **Seleccionar o deseleccionar todo** para aplicar los cambios a todos o a ninguno de los módulos de E/S.

   o

   Active la casilla de las ranuras específicas para seleccionar los módulos de E/S requeridos.
5. En la sección **Editar VLAN**, seleccione **Actualizar las VLAN sin etiquetar** en la lista desplegable y haga clic en **Aplicar**.
   Se mostrará un mensaje de advertencia que indica que la configuración de la VLAN sin etiquetar existente se sobrescribirá con la configuración de la VLAN sin etiquetar recientemente asignada.
6. Haga clic en **Aceptar** para confirmar.
   Las VLAN sin etiquetar se actualizarán con las configuraciones de la VLAN sin etiquetar recientemente asignada.

   Aparecerá el mensaje Operación satisfactoria. La configuración actual de las VLAN asignadas a los módulos de I/O se mostrará en el campo Resumen de asignaciones de VLAN.

Restablecimiento de las VLAN para los módulos de E/S mediante la interfaz web de la CMC

Para restablecer las VLAN para los módulos de E/S a las configuraciones predeterminadas mediante la interfaz web de la CMC:

1. Vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración** > **Administrador de VLAN**.
   Aparecerá la página Administrador de VLAN.
2. En la sección **Seleccionar módulo de E/S**, seleccione los módulos de E/S requeridos.
3. En la sección **Editar VLAN**, seleccione **Restablecer VLAN** en la lista desplegable y haga clic en **Aplicar**.
   Se mostrará un mensaje que indica que las configuraciones de las VLAN existentes se sobrescribirán con las configuraciones predeterminadas.
4. Haga clic en **Aceptar** para confirmar.
   Las VLAN se asignarán a los módulos de E/S seleccionados de acuerdo con las configuraciones predeterminadas.

   Aparecerá el mensaje Operación satisfactoria. La configuración actual de las VLAN asignadas a los módulos de I/O se mostrará en el campo Resumen de asignaciones de VLAN.

NOTA: La opción **Restablecer todas las VLAN** no se admite en agregadores de E/S en el modo Enlace troncal de enlace virtual - VLT.

16

Administración y supervisión de la alimentación

El chasis Dell PowerEdge FX2/FX2s es el gabinete de servidor modular más eficiente 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.

La administración de energía en PowerEdge FX2/FX2s es relativamente diferente de los de PowerEdge VRTX. Uno de los cambios principales en la administración de energía técnica es el uso de un sistema de bucle cerrado del acelerador (CLST) para mantener el límite de alimentación del chasis deseado. El propósito de utilizar esta técnica es que, tiene un mejor control y también permite que el chasis utilice por completo las PSU disponibles.

Las funciones de administración de la alimentación de PowerEdge FX2/FX2s 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 PowerEdge FX2/FX2s consume energía de CA y distribuye la carga a través de la unidad de suministro de energía (PSU) activa. El sistema puede producir hasta 3371 vatios de energía de CA y asignarlos a módulos de servidor y a la infraestructura de gabinete asociada. No obstante, esta capacidad puede variar en función de la política de redundancia de alimentación que seleccione.

El gabinete PowerEdge FX2/FX2s se puede configurar para cualquiera de las tres 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.

También puede controlar la administración de la 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

El centro OMPC administra, entonces, lo siguiente:

- Alimentación del servidor
- Capacidad de alimentación de entrada del sistema

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 el estado del chasis, los servidores y 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:

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:

- Redundancia de cuadrícula
- No redundancia
- Solo alertas de redundancia

Política de redundancia de la red eléctrica

La política de redundancia de la red eléctrica también se conoce como política 1+1, para una unidad de suministro de energía activa y una de repuesto.

El objetivo de la política de redundancia de la red eléctrica es permitir que un sistema de gabinete funcione de modo que le permita al gabinete 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 (PSU). Cuando configure un sistema para la redundancia de la red eléctrica, conecte las PSU 1 y 2 a redes eléctricas independientes.

En este modo, la CMC garantiza que el consumo de alimentación se mantenga de modo que el sistema siga funcionando sin degradación si se produce un error en alguna de las redes eléctricas o en una sola unidad de suministro de energía. El encendido del servidor se limita a la alimentación disponible de una sola PSU. Si en cualquier momento no se puede mantener la redundancia (como, por ejemplo, si se extrae o falla una PSU) se generarán alertas y el estado del chasis pasará a **Crítico**.

Sin política de redundancia

La política Sin redundancia también se conoce como política de 2+0.

En este modo, toda la potencia de las dos unidades de suministro de energía está disponible y se utiliza, pero no se garantiza que la falla de una unidad de suministro de energía o de la red eléctrica no afecten el funcionamiento del sistema.

Política Alertas de redundancia únicamente

La política Alertas de redundancia únicamente le permite al encendido del servidor utilizar la capacidad de ambas PSU mientras se generan alertas sobre condiciones reales, tales como la eliminación o falla de una PSU o cuando el consumo real de alimentación excede las capacidades de una sola PSU. Esta es la política predeterminada.

Modo de tolerancia a errores

Esta política utiliza los límites de capacidad de alimentación de una única unidad del sistema de alimentación (PSU) de manera similar a la política de redundancia de la cuadrícula. En este modo, la alimentación pico de los subsistemas de la CPU se reemplaza por un nuevo límite IccMax. Esta política se aplica únicamente a la 14ª generación de servidores blade de Dell.

Errores de unidad de suministro de energía

Los errores de la unidad de suministro de energía de cualquier tipo siempre se advierten, independientemente de la política de redundancia seleccionada.

NOTA: Modificar la política de redundancia del gabinete modular mientras el gabinete está apagado.

Configuración predeterminada de redundancia

Solo alertas de redundancia es la configuración predeterminada de redundancia de un chasis y dos unidades de suministro de energía (PSU).

Adaptación del sled de nodos múltiples

El PowerEdge FM120x4 es un sled de múltiples nodos y ancho medio que puede incluir cuatro servidores con el iDRAC asociado con procesadores independientes. Está diseñado para alcanzar una eficiencia de alimentación óptima y los procesadores no se pueden quitar. Los procesadores de PowerEdge FM120 comparten la misma infraestructura de alimentación, por ejemplo, un solo sensor de temperatura y alimentación para todo el sled.

Supervisión del límite de alimentación del chasis

OpenManage Power Center (OMPC) se puede utilizar para supervisar y controlar el consumo de alimentación de las máquinas en un centro de datos. PowerEdge FX2/FX2s permite el OMPC al proporcionar un aprovisionamiento para establecer el límite de alimentación para el chasis, y límites para guiar el valor del límite de alimentación. Los límites superiores e inferiores de alimentación se establecen por medio de la CMC y no se pueden configurar.

NOTA: El límite inferior es la alimentación mínima necesaria para hacer funcionar el chasis en función de la configuración actual. El límite superior refleja el máximo nivel de alimentación disponible en la política de redundancia actual.

NOTA: Si el Modo máximo de conservación de energía (MPCM) se encuentra activado en el chasis, todas las solicitudes de alimentación de un servidor blade se rechazan. El servidor blade no se encuentra encendido si existe alguna acción en el iDRAC o el servidor blade que requiera que el host inicie el ciclo de encendido.

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 de la 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 mediante 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
```

Visualización del estado de presupuesto de alimentación mediante la interfaz web de la 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 haga clic en **Alimentación** > **Estado de presupuesto**. La página **Estado del presupuesto de alimentación** muestra la configuración de la política de alimentación del sistema con los atributos **Límite de alimentación de entrada del sistema**, **Política de redundancia**, los detalles del presupuesto de alimentación con los atributos **Capacidad máx. de alimentación de entrada del sistema**, **Reserva de redundancia de entrada**, **Alimentación disponible para el encendido del servidor**) y suministro de energía del chasis

con los detalles de la unidad de la fuente de alimentación. Para obtener más información, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

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 *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

Estado de redundancia y condición general de la alimentación

El estado de redundancia es un factor para determinar el estado general de alimentación. Cuando la política de redundancia de alimentación está configurada, por ejemplo, en Redundancia de red y el estado de redundancia indica que el sistema está funcionando con redundancia, el estado general de alimentación suele ser **Correcta**. Si la PSU instalada en un chasis falla debido a algún motivo, el estado general de alimentación del chasis se muestra como **No crítico**. Sin embargo, si no se pueden cumplir las condiciones para operar con redundancia de cuadrícula, el estado de redundancia es **No** y el estado general de alimentación es **Crítico**. Esto se debe a que el sistema no puede funcionar de acuerdo con la política de redundancia configurada.

El CMC activo sondea el estado de CMC en espera para determinar si el chasis es redundante. Si desconecta el cable de red, se activará una conmutación por error del chasis después de 30 segundos. Luego, el CMC en espera se activa. La interrupción de red hace que la CMC activo originalmente arranque después de aproximadamente tres minutos y se convierta en una CMC en espera. La tarea de monitoreo de estado en el CMC en espera se reanuda después de cinco minutos. Los cambios de estado, si los hubiera, en el modo de espera se procesan solo después de que el estado de espera sea estable. El CMC activo debe esperar durante ocho minutos y medio para determinar si existe redundancia. Asegúrese de que el estado de redundancia presente buenas condiciones antes de iniciar una conmutación por error debido a cambios de estado.

NOTA: CMC no realiza una comprobación previa de estas condiciones cuando cambia la política de redundancia a redundancia de red o desde este modo a otro. Por lo tanto, es posible que la configuración de la política de redundancia provoque una pérdida o recuperación de la condición de redundancia.

Administración de la alimentación tras una falla de la unidad de suministro de energía

En el caso de que se produzca una falla o eliminación de una PSU, se puede reducir la alimentación suministrada a los servidores. En casos extremos, los servidores se pueden apagar en un intento de mantener el funcionamiento. La configuración y el mantenimiento de la Redundancia de la cuadrícula evita que los servidores se vean afectados por la falla de una única PSU.

Cambios de suministro de energía y política de redundancia en el registro de sucesos del sistema

Los cambios en el estado de la fuente de alimentación y la política de redundancia de alimentación se registran como sucesos. Los eventos relacionados con la fuente de alimentación que registran anotaciones en el registro de eventos del sistema (SEL) son inserción y extracción de fuentes de alimentación, inserción y extracción de entrada de fuentes de alimentación, y declaración y retiro de declaración de salida de fuentes de alimentación.

La siguiente tabla incluye las anotaciones en el SEL que están relacionadas con los cambios en el suministro de energía:

Tabla 27. 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.
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 que está configurado para una política de alimentación de **Redundancia de la red eléctrica** o para una política de **Sólo alertas de redundancia**. En la tabla siguiente se enumeran las anotaciones del SEL relacionadas con los cambios en la política de redundancia de alimentación.

Tabla 28. Eventos 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, módulos de E/S, CMC, PCIe y a la infraestructura del chasis). 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
- Desactivar botón de encendido del chasis
- Modo de conservación máx. de alimentación
- Registro remoto de la alimentación
- Intervalo del registro remoto de la alimentación
- Desactivar restablecimiento de la alimentación de CA

Conservación de la energía y presupuesto de alimentación

Si el uso de energía supera el Límite de alimentación de entrada del sistema, la energía que se suministra a los servidores por la unidad de suministro de energía se reducirá para mantener el nivel nominal.

Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web de la 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 información acerca de los distintos campos, consulte la *Ayuda en línea*.
   - **Política de redundancia**

- **Desactivar botón de encendido del chasis**
- **Modo de conservación máx. de 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 0 (Sin redundancia), 1 (Redundancia de la red eléctrica) y 3 (Solo alertas de redundancia). El valor predeterminado es 3.

     Por ejemplo, el siguiente comando establece la política de redundancia en:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisRedundancyPolicy 1
     ```

   - Para establecer el valor del presupuesto de alimentación, escriba:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPowerCap <value>
     ```

     donde <*value*> es un número entre la carga del chasis de tiempo de ejecución actual y 3371, lo cual representa el límite de energía máximo en vatios. El valor predeterminado es 3371.

     Por ejemplo, el siguiente comando establece el presupuesto máximo de la alimentación en 3371 vatios:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPowerCap 3371
     ```

   - Para ver el límite superior y límite inferior, especifique lo siguiente:

     ```
     racadm getconfig -g cfgchassispower -o cfgchassispowercap <lower,upper> bound
     ```

     donde <*lower, upper*> es el límite superior y límite inferior.

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPowerCap 3000
     ```

   - 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 los registros de sistemas remotos se hayan configurado anteriormente. Se debe activar el registro en uno o más hosts de los registros de sistemas remotos; de lo contrario, se registra el consumo de energía. Esto se puede hacer mediante la GUI web o la CLI de RACADM. Para obtener más información, consulte las instrucciones de configuración del registro del sistema remoto.
- 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 RACADM para la alimentación del chasis, consulte las secciones **config**, **getconfig**, **getpbinfo** y **cfgChassisPower** en la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

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).

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 general 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 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**
   - **Apagado ordenado**
   - **Encender el servidor**
   - **Apagar el servidor**
   - **Restablecer el servidor (reinicio mediante sistema operativo)**
   - **Ciclo de encendido del servidor (reinicio mediante suministro de energía)**

   Para obtener información acerca de las opciones, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.
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).

   NOTA: Los servidores blade modulares se encuentran en estado de regulación durante un reinicio o una conmutación por error de la CMC.

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 control 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.

Para obtener más información sobre los comandos RACADM, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s.* disponible en dell.com/support/manuals.

Configuración del botón de encendido del Sled

Puede configurar el botón de alimentación del Sled para que esté desactivado, de modo que cuando presione el botón de alimentación del Sled no ocurra nada. Para configurar el botón de alimentación del Sled, vaya a **Descripción general del chasis** > **Descripción general del servidor** > **Alimentación** > **Control**.

En la sección **Propiedad**, seleccione la casilla de verificación para desactivarlo o deseleccione la casilla para activarlo.

NOTA: Esta configuración se aplica solamente a los Sleds de múltiples nodos presentes en el chasis. El resto de los Sleds no se verán afectados.

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.

17

Configuración de las ranuras PCIe

El chasis PowerEdge FX2/FX2s contiene opcionalmente ocho ranuras PCIe y cada ranura PCIe se asigna a un sled específico. De manera predeterminada, todas las ranuras PCIe están asignadas. Puede activar o desactivar la asignación de ranuras PCIe a los servidores mediante la interfaz web de la CMC o los comandos RACADM.

Las siguientes tablas detallan las asignaciones de PCIe para sleds de cálculo de ancho completo, de medioa ancho y de cuarto de ancho.

Tabla 29. Asignación de PCIe para sleds de cálculo de ancho completo

Ranura PCIe	Asignación para sleds de ancho completo (PowerEdge FC830)
Ranura-1 de PCIe	3
Ranura-2 de PCIe	3
Ranura-3 de PCIe	1
Ranura-4 de PCIe	1
Ranura-5 de PCIe	3
Ranura-6 de PCIe	3
Ranura-7 de PCIe	1
Ranura-8 de PCIe	1

Tabla 30. Asignación de PCIe para sleds de cálculo de medio ancho

Ranura PCIe	Asignación para sleds de medio ancho (PowerEdge FC630)
Ranura-1 de PCIe	4
Ranura-2 de PCIe	4
Ranura-3 de PCIe	2
Ranura-4 de PCIe	2
Ranura-5 de PCIe	3
Ranura-6 de PCIe	3
Ranura-7 de PCIe	1
Ranura-8 de PCIe	1

Tabla 31. Asignación de PCIe para sleds de cálculo de un cuarto de ancho

Ranura PCIe	Asignación para sleds de un cuarto de ancho (PowerEdge FC430)
Ranura-1 de PCIe	3d
Ranura-2 de PCIe	3c
Ranura-3 de PCIe	1d
Ranura-4 de PCIe	1c
Ranura-5 de PCIe	3b
Ranura-6 de PCIe	3a
Ranura-7 de PCIe	1b
Ranura-8 de PCIe	1a

NOTA: La administración de PCIe sólo se admite para PowerEdge FX2s y no para PowerEdge FX2.

Para obtener más información sobre la asignación de ranuras PCIe, consulte el *Dell PowerEdge FC332 Owner's Manual* (Manual del propietario de Dell PowerEdge FD332)

Para obtener más información sobre la administración de ranuras PCIe, consulte la *Ayuda en línea de la CMC para Dell PowerEdge FX2/FX2s*.

NOTA: La función de supervisión sin agentes no está disponible para las tarjetas de red y PCIe de PERC en las ranuras PCIe del chasis. Esta función es la solución de administración de sistemas para los servidores PowerEdge de 12da generación de Dell. Se realiza fuera de banda sin depender de agentes del sistema operativo. Mediante la supervisión sin agentes, puede supervisar el almacenamiento conectado a los dispositivos de red del servidor (PERC, discos duros, gabinetes, etc.) mediante iDRAC, sin tener que instalar un agente en el sistema administrado o la estación de administración. Para obtener más información sobre la supervisión sin agentes, consulte el artículo *Inventario y supervisión sin agentes para almacenamiento y dispositivos de red en los servidores PowerEdge 12G de Dell* en **Dell TechCenter**.

Temas:

Visualización de propiedades de ranuras PCIe mediante la interfaz web de la 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 de 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**.

Visualización de propiedades de ranuras PCIe mediante RACADM

Es posible ver una asignación de ranura PCIe a un servidor mediante los comandos RACADM. Aquí se presentan algunos de estos comandos. Para obtener más información acerca de los comandos RACADM, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/manuals**.

NOTA: El nombre de la tarjeta PCIe solo se mostrará después de que el BIOS complete el `POST` en el Sled asociado. Hasta entonces, el nombre del dispositivo aparecerá como **Desconocido**.

- Para ver la asignación actual de dispositivos PCIe a servidores, ejecute el siguiente comando:

```
racadm getpciecfg -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
```

- Si desea ver los valores de configuración de PCIe existentes, ejecute el siguiente comando:

```
racadm getconfig -g cfgPCIe
```

NOTA: La tarjeta PCIe no está encendida si la tarjeta secundaria no está presente en el Sled asociado.

Reasignación de PCIe

La función Reasignación de PCIe permite asignar ranuras PCIe asignadas a los sleds de cálculo en los compartimentos inferiores a los sleds de cálculo de los compartimentos superiores..

Puede activar o desactivar la opción de reasignación de PCIe mediante la interfaz web de la CMC, CMC WSMAN o RACADM. Debe tener el privilegio de configuración del chasis para configurar o modificar la configuración de reasignación. Apague todos los sled de cálculo en el chasis antes de modificar la configuración de reasignación. Cuando se encienden los sled de cálculo después de que cambia la reasignación, las ranuras asignadas a los sled de cálculo en la bahía inferior anterior se asignan a los sled de cálculo correspondientes en la bahía superior. A continuación, se mencionan algunos ejemplos de reasignación de PCIe:

- **Reasignación de PCIe en FC830 de ancho completo (FW):**
  - Las ranuras de PCIe asignadas al sled-3 (ranuras de PCIe 1 a 4) de FW se reasignan al sled-1. El sled-1 ahora se asigna a las ranuras de PCIe 1 a 8.
- **Reasignación de PCIe en FC630 de medio ancho (HW):**
  - Las ranuras de PCIe asignadas al sled-3 (ranuras de PCIe 5 y 6) de HW se reasignan al sled-1. El sled-1 ahora se asigna a las ranuras de PCIe 5 a 8.
  - Las ranuras de PCIe asignadas al sled-4 (ranuras de PCIe 1 y 2) de HW se reasignan al sled-2. El sled-2 ahora se asigna a las ranuras de PCIe 1 a 4.
- **Reasignación de PCIe en FC430 de un cuarto de ancho (QW):**
  - La ranura de PCIe asignada al sled-3a (ranura de PCIe 6) de QW se reasigna al sled-1. El sled-1a ahora se asigna a las ranuras de PCIe 6 y 8.
  - La ranura de PCIe asignada al sled-3b (ranura de PCIe 5) de QW se reasigna al sled-1b. El sled-1b ahora se asigna a las ranuras de PCIe 5 y 7.
  - La ranura de PCIe asignada al sled-3c (ranura de PCIe 2) de QW se reasigna al sled-1c. El sled-1c ahora se asigna a las ranuras de PCIe 2 y 4.
  - La ranura de PCIe asignada al sled-3d (ranura de PCIe 1) de QW se reasigna al sled-1d. El sled-1d ahora se asigna a las ranuras de PCIe 1 y 3.

Para obtener más información, consulte el *Manual del propietario de gabinetes Dell PowerEdge FX2 y FX2s*.

Activación o desactivación de reasignaciones de PCIe mediante la interfaz web de la CMC

1. En el panel izquierdo, haga clic en **Descripción general de PCIe.**
   Aparecerá la página **Estado de PCIe**.
2. Haga clic en **Configuración**.
   Aparecerá la página **Asignación: reasignación de ranura PCIe**.
3. Seleccione o deseleccione la casilla de verificación **Activar reasignación de ranura PCIe** y haga clic en **Aplicar**.

Activación o desactivación de reasignaciones de PCIe mediante RACADM

Los valores de entrada para activar o desactivar la reasignación de PCIe a una ranura son:

- 1: Habilitar
- 0: Inhabilitar

Para activar una reasignación de PCIe, ejecute el siguiente comando:

```
racadm config -g cfgPCIe -o cfgPCIeReassignmentEnable 1
```

Para desactivar una reasignación de PCIe, ejecute el siguiente comando:

```
racadm config -g cfgPCIe -o cfgPCIeReassignmentEnable 0
```

Para obtener más información, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s* disponible en **dell.com/support/Manuals**.

18

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.

Temas:

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 eventos.

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 RACADM. Para obtener más información sobre `racdump`, consulte la *Guía de referencia de la línea de comandos RACADM de Dell Chassis Management Controller para PowerEdge FX2/FX2s*.

Tabla 32. 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 del NIC (módulo CMC)	`getniccfg`
Información del registro de rastreo	`gettracelog`
Registro de sucesos de RAC	`getraclog`
Registro de sucesos del sistema	`getsel`

Descarga del archivo MIB (Base de información de administración) SNMP

El archivo Base de información de administración (MIB) SNMP de la CMC define los tipos de chasis, eventos e indicadores. La CMC permite descargar el archivo MIB a través de la interfaz web.

Para descargar el archivo Base de información de administración (MIB) 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 de suministro de energía en el lado 1 (ranura izquierda) y suministro de energía en el lado 2 (ranura derecha) para estar presente y en estado funcional en el gabinete. Asimismo, la capacidad de cada suministro debe ser suficiente para soportar todas las asignaciones de energía necesarias para que el chasis mantenga **Redundancia de cuadrícula**.
  - **Solución B:** revise si todos los suministros de energía están conectados correctamente a las dos redes de CA. El suministro del lado 1 debe estar conectado a una cuadrícula de CA y el del lado 2 debe estar conectado a la otra cuadrícula, y ambas cuadrículas de CA deben estar en funcionamiento. La **Redundancia de cuadrícula** se pierde cuando una de las cuadrículas 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:** verifique y reemplace el cable de CA. Verifique y confirme que la unidad de distribución de energía que proporciona la alimentación al suministro funcione como se espera. Si no se soluciona el error, comuníquese con el servicio de 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:** 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.
- **Problema:** la alimentación disponible cambia continuamente, incluso si no ha cambiado la configuración de gabinete.
  - **Solución:** el 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:** 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 hardware de eventos que ocurren en el chasis. Para ver el registro de hardware, utilice la interfaz web y el 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.

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 del registro del chasis

El CMC genera un registro de los sucesos relacionados con el chasis.

NOTA: Para borrar el registro del chasis, debe tener privilegios de **Administrador de borrado de registros**.

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 o volver a restablecer virtualmente los servidores de modo tal que se comporten como si se los hubiese quitado y vuelto a insertar.

NOTA: Para restablecer componentes, debe tener privilegios de **Administrador de comandos de depuración**.

NOTA: El restablecimiento virtual no está disponible para los nodos individuales de la PowerEdge FM120x4.

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, en la sección **Estado de la CMC**, haga clic en **Restablecer la CMC**. La CMC disponible se reinicia.

Para obtener más información, consulte la *Ayuda en línea del CMC para Dell PowerEdge FX2/FX2s*.

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:

NOTA: La información de Flexaddress, perfiles de servidor y almacenamiento extendido no se guardan ni se restauran con la configuración del chasis. Se recomienda guardar los perfiles del servidor que son importantes separados del chasis mediante un recurso compartido de archivos remoto o una copia guardada en una estación de trabajo local. Para obtener más detalles sobre cómo realizar esta operación, consulte Agregar o guardar perfil

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**. Sustituya la ruta 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 únicamente para este chasis.
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 la nueva o modificada configuración. Una vez que el proceso se complete correctamente, se cerrarán todas las sesiones actuales.

Solución de errores de protocolo de hora de red

Después de configurar la CMC para sincronizar el reloj con un servidor de hora remoto a través de la red, pueden transcurrir de 2 a 3 minutos hasta de que se produzca un cambio en la fecha y la hora. Si transcurrido este tiempo no se produce ningún cambio, es posible que se deba 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 del Servidor de Protocolo de hora de red (NTP) 1, el Servidor NTP 2 y el 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 NTP, consulte 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
```

Si no se muestra el símbolo '*' en alguno de los servidores configurados, es posible que los valores no se hayan configurado correctamente. 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 alto 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 ingresar 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 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 CMC_Stmp_Configuración de los LED para identificar componentes en el chasis.

Tabla 33. Colores y patrones de parpadeo de los LED

Componente	Color de LED, patrón de parpadeo	Estado
CMC		Encendido
		Apagado
	Azul, encendido permanentemente	Se está cargando el firmware El firmware se actualizó correctamente
	Apagado	La actualización del firmware está en curso
	Azul, encendido permanentemente	Activo
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
Servidor		Encendido
		Se está cargando el firmware
		Apagado
	Azul, encendido permanentemente	El servidor está seleccionado en el KVM
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas
Módulo de I/O (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 I/O (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

Tabla 33. Colores y patrones de parpadeo de los LED (continuación)

Componente	Color de LED, patrón de parpadeo	Estado
	Azul, apagado	Sin fallas
Ventilador	Verde, encendido permanentemente	Ventilador funcionando
	Verde, parpadeante	No se utiliza
	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
PCI	Azul, apagado	Encendido
	Azul, parpadeante	La identificación PCI está en curso.
	Ámbar, parpadeante	Falla
Sled de almacenamiento	Ámbar, parpadeante	Falla
	Azul sólido	Sin fallas

Solución de problemas de un CMC que no responde

Si no puede iniciar sesión en CMC por medio de alguna de las interfaces (interfaz web, Telnet, SSH, RACADM remoto o serie), puede verificar la funcionalidad de CMC con los indicadores LED en CMC.

Observación de los LED para aislar el problema

La CMC cuenta con un LED que cambia de color para indicar:

Tabla 34. Indicadores de color de LED

Color	Descripción
Azul	Funcionamiento normal
Azul, parpadeante	ID (0,5 segundos encendido, 0,5 segundos apagado)
Ámbar	Resumen del error del chasis
Ámbar, parpadeante	Error de chasis con Identificación simultánea

Solución de problemas de red

El registro de rastreo interno de la CMC le permite depurar las alertas y las redes de la CMC. Puede acceder al registro de rastreo mediante la interfaz web de la CMC o RACADM. Consulte la sección del comando `gettracelog` en la *Guía de referencia de la línea de comandos RACADM para iDRAC y CMC*.

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 del CMC que están relacionados con el firmware interno del CMC, no con el sistema operativo del sistema administrado.

Solución de problemas generales

Cuando aparece un mensaje de ejecución satisfactoria una vez finalizada una operación, como guardar un perfil de servidor, a veces la acción puede no tener efecto.

Para resolver este problema, verifique si alguno de los puertos de servicio de la CMC para SSH, Telnet, HTTP o HTTPS usa los puertos usados comúnmente por los servicios del SO, como 111. Si es utilizado por los puertos de servicio de la CMC, cambie la configuración a un puerto no reservado. Para obtener más información sobre los puertos reservados, visite http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Solución de problemas del módulo de almacenamiento en el chasis FX2

La siguiente información le ayuda a solucionar problemas relacionados con los sleds de almacenamiento en el chasis FX2.

- **Problema:** no se detecta el módulo de almacenamiento al insertarlo. No se detectan el módulo de almacenamiento insertado ni el servidor asociado encendido

  Resolución: asegúrese de realizar un ciclo de encendido en el servidor asociado después de insertar el módulo de almacenamiento.

- **Problema:** el módulo de almacenamiento está insertado y se ha realizado un ciclo de encendido en el servidor asociado pero no se detecta el módulo.

  Resolución: verifique el registro del chasis para obtener más información sobre la falla. Verifique si existe alguna falla en el hardware, como la falta de detección de un desplazamiento de cable o RAID.

- **Problema:** el LED ámbar de almacenamiento parpadea.

  Solución: asegúrese de que el módulo de almacenamiento esté insertado correctamente y verifique si hay mensajes de advertencia en el registro del chasis. Este error se puede solucionar únicamente si se soluciona la falla subyacente y se realiza un ciclo de encendido en el host asociado con el sled extraído o a través de un restablecimiento virtual del sled.

  Problema: la actualización del firmware de RAID del módulo de almacenamiento no resulta eficiente.

  Resolución: si está en modo dual dividido del host, se debe realizar un ciclo de encendido en cada host conectado a RAID del sled de almacenamiento para que el cambio de firmware de RAID surta efecto.

- **Problema:** la opción Reasignación de ranura PCIe está desactivada en la interfaz gráfica de usuario.

  Solución: asegúrese de que todos los hosts del chasis estén encendidos. Si intenta cambiar esta configuración desde RACADM mientras un host está encendido, aparecerá un mensaje de error. Se debe tener privilegio de administrador de configuración del chasis para cambiar esta configuración.

- **Problema:** la Reasignación de ranura PCIe está activada y el host está encendido pero las ranuras PCIe no están encendidas.

  Resolución: verifique el registro del chasis para ver mensajes de advertencia asociados con BIOS o iDRAC no actualizados o con host o no admitido.

- **Problema:** no es posible importar, exportar, ni eliminar las licencias del módulo de almacenamiento.

  Resolución: se debe tener privilegio de configuración del chasis para importar, exportar y borrar las licencias del módulo de almacenamiento.

Restablecimiento de la contraseña olvidada del administrador.

PRECAUCIÓN: Muchas de las reparaciones deben ser realizadas únicamente por un técnico de servicio autorizado. Realice reparaciones simples y solución de problemas según lo autorizado en la documentación del producto o según lo indique el equipo de servicio y soporte telefónico o en línea. Los daños causados por reparaciones no autorizadas por Dell no están cubiertos por la garantía. Lea y siga las instrucciones de seguridad que se incluyen con el producto.

Para realizar acciones de administración, se requiere un usuario con privilegios de **Administrador**. El software de la CMC cuenta con una función de seguridad de protección con contraseña de la cuenta de usuario, la cual se puede desactivar si olvida la contraseña de la cuenta de administrador. Si olvida la contraseña de la cuenta de administrador, puede recuperarla mediante el puente J_PWORD en la placa de la CMC.

La placa de la CMC cuenta con un conector de dos pines de restablecimiento de contraseña, como se muestra en la siguiente figura. Si hay un puente instalado en el conector de restablecimiento, se habilitan la contraseña y la cuenta predeterminadas de administrador y se configuran con los valores predeterminados de `username: root` y `password: calvin`. La cuenta del administrador se restablecerá, sin importar si se eliminó la cuenta o se cambió la contraseña.

NOTA: Asegúrese de que el módulo de la CMC esté en estado pasivo antes de comenzar.

Para realizar acciones de administración, se requiere un usuario con privilegios de **Administrador**. Si olvida la contraseña de la cuenta de administrador, puede restablecerla mediante el puente J_PWORD en la placa de la CMC.

El puente PASSWORD_RST utiliza un conector de dos clavijas, tal como se muestra en la siguiente figura.

Mientras el puente PASSWORD_RST está instalado, la cuenta y contraseña predeterminadas del administrador están activadas y se definen con los siguientes valores predeterminados:

```
username: root
password: calvin
```

La cuenta del administrador se restablecerá de forma temporal, independientemente de que se haya eliminado la cuenta o se haya cambiado la contraseña.

NOTA: Cuando el puente PASSWORD_RST está instalado, se utiliza una configuración de consola serie predeterminada (y no valores de propiedades de configuración), tal como se indica a continuación:

```
cfgSerialBaudRate=115200
cfgSerialConsoleEnable=1
cfgSerialConsoleQuitKey=^\
cfgSerialConsoleIdleTimeout=0
cfgSerialConsoleNoAuth=0
cfgSerialConsoleCommand=""
cfgSerialConsoleColumns=0
```

1. Presione el pestillo de liberación de CMC en el asa y sepárelo del panel frontal del módulo. Extraiga el módulo CMC del alojamiento.

   NOTA: Las descargas electrostáticas (ESD) pueden dañar la CMC. En determinadas condiciones, se puede acumular ESD en su cuerpo o en un objeto, la cual luego se descarga en la CMC. Para evitar daños por ESD, tome las precauciones necesarias para descargar la electricidad estática de su cuerpo cuando maneje y acceda a la CMC fuera del chasis.

2. Retire el conector de puente del conector de restablecimiento de contraseña e inserte un puente de dos pines para activar la cuenta de administrador predeterminada. Para localizar el puente de contraseña en la placa de la CMC, consulte la siguiente figura.

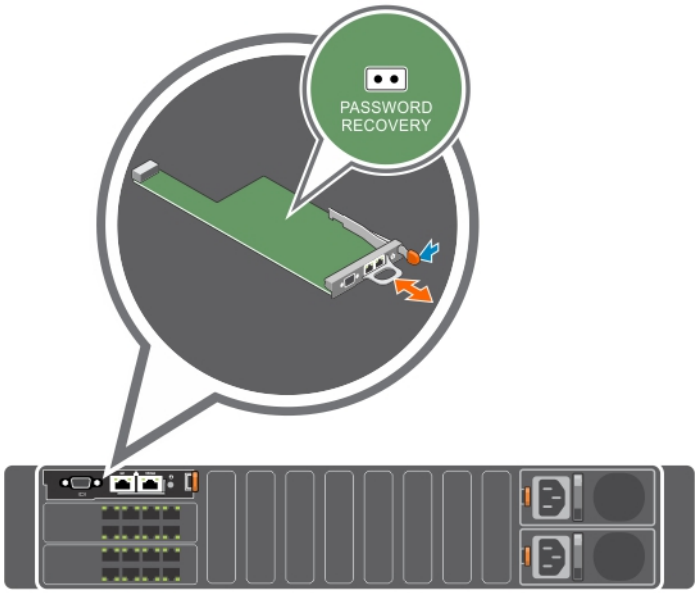


Tabla 35. Opciones del puente de contraseña del CMC

Comando de puente	Imagen del puente	Estado del puente	Estado de restablecimiento del puente
J_PWORD		(predeterminada)	La función de restablecimiento de contraseña está desactivada.
			La función de restablecimiento de contraseña está activada.

3. Inserte el módulo CMC en el gabinete. Vuelva a conectar los cables que se desconectaron.

   NOTA: Asegúrese de que el módulo de la CMC está activo hasta finalizar los pasos restantes.

4. Espere que la CMC termine de reiniciarse. En la interfaz web, en el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Alimentación** > **Control**, seleccione **Restablecer CMC (inicio mediante sistema operativo)** y haga clic en **Aplicar**.
5. Inicie sesión en la CMC activa con el nombre de usuario y la contraseña predeterminados de administrador (root y calvin) y restaure la configuración de cuenta de usuario que necesite. Las cuentas y contraseñas existentes no se deshabilitan y permanecen activas.
6. Realice las acciones de administración requeridas, que incluyen la creación de una nueva contraseña de administrador.
7. Quite el puente de dos clavijas PASSWORD_RST y vuelva a colocar el tapón del puente.
   a. Presione el pestillo de liberación de CMC en el asa y sepárelo del panel frontal del módulo. Extraiga el módulo CMC del alojamiento.
   b. Quite el puente de dos clavijas y vuelva a colocar el tapón del puente.
   c. Inserte el módulo CMC en el gabinete. Vuelva a conectar los cables que se desconectaron. Repita el paso 4 para que el módulo CMC no puenteado sea la CMC activa.

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
- 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 local: problemas de sintaxis, errores tipográficos y nombres incorrectos. 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. Aparece el siguiente mensaje de error

```
racadm command failed.
```

Para ver información sobre un chasis, ingrese 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` al utilizar los comandos `$ logout` y `$ quit`.

Administración y recuperación de un sistema remoto

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 la 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 navegador web muestra una advertencia de seguridad al emitir el certificado predeterminado para un certificado predeterminado de la CMC que no coincide con el nombre del host de la CMC (por ejemplo, la dirección IP).

Para solucionar este problema de seguridad, cargue un certificado de servidor de la CMC que haya sido emitido para 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**.

¿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 la 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 solucionar este problema de seguridad, cargue un certificado de servidor de la CMC que haya sido 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 del descubrimiento, IT Assistant intenta verificar los nombres de comunidad **Obtener** y **Establecer** del dispositivo. En IT Assistant, **Obtener nombre de comunidad = público** y **Establecer nombre de comunidad = privado.** De manera predeterminada, el nombre de comunidad para el agente 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 utilizando 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, ingrese nombres de comunidad de entrada aceptados por el agente. Como el CMC solo permite un nombre de comunidad, ingrese el mismo nombre de comunidad Obtener y Establecer para la configuración de descubrimiento de IT Assistant.

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 el modo Windows 2003. Asimismo, los grupos entre el Objeto de asociación, los Objetos de usuario de RAC y los Objetos de dispositivos 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 de Dell permite crear únicamente estos dos objetos en el mismo dominio. Otros objetos pueden estar en dominios diferentes.

¿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 el 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}
```

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 conmutador. Si se comete un error al configurar la IP/máscara/puerta de enlace, el conmutador 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.

Sucesos y mensajes de error

Después de degradar el firmware de la CMC desde la versión más reciente a versiones anteriores, ¿por qué muestra el registro del chasis el siguiente mensaje para algunos de los registros?

```
USR8513 - MessageID missing from message registry.
```

Lo que ve es un nuevo mensaje introducido en el firmware actual que indica que el firmware anterior no puede interpretar. Para obtener más información sobre la ID del mensaje, consulte la *Guía de referencia de eventos y mensajes de error* en OpenManage Software en **www.dell.com/openmanagemanuals**.