Dell Chassis Management Controller versión 6.0 para PowerEdge M1000e

Guía del usuario

Septiembre 2017
Rev. A02

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, Controladora de administración de chasis Dell) para chasis Dell PowerEdge M1000e es una solución de hardware y software de administración de sistemas para administrar varios chasis de servidores Dell. Es una tarjeta de acoplamiento activo que se instala en la parte posterior del chasis Dell PowerEdge M1000e. La CMC cuenta con su propio microprocesador y memoria y recibe energía del chasis modular al que está conectado.

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

- Ver el inventario
- Realizar tareas de configuración y supervisión
- Encender o apagar remotamente servidores
- Activar alertas para los sucesos en los servidores y los componentes en el chasis del M1000e

El chasis M1000e se puede configurar con una sola CMC o con CMC redundantes. En las configuraciones de CMC redundantes, si la CMC principal pierde la comunicación con el chasis M1000e o la red de administración, la CMC en espera asume la administración del chasis.

La CMC proporciona varias funciones de administración de sistemas para servidores. La administración térmica y la administración de alimentación son las funciones principales de la CMC.

- Administración térmica y de energía automática en tiempo real de nivel de alojamiento.
  - La CMC supervisa los requisitos de alimentación del sistema y admite el modo opcional de conexión dinámica de suministros de energía. Este modo permite que la CMC mejore la eficiencia energética, al configurar los suministros de energía en espera según los requisitos de carga y de redundancia.
  - El CMC informa el consumo de energía en tiempo real, lo que incluye el registro de los puntos máximos y mínimos con una indicación de hora.
  - La CMC permite fijar un límite de alimentación máxima opcional para el gabinete, que avisará o realizará alguna acción, tal como regular los módulos de servidor o evitar que se enciendan nuevos servidores blade para mantener el gabinete por debajo del límite.
  - El CMC supervisa y controla automáticamente los ventiladores de refrigeración en función de mediciones reales de la temperatura interna y ambiente.
  - El CMC proporciona informes completos de errores o de estado y del inventario del gabinete.
- El CMC proporciona un mecanismo para configurar de forma centralizada lo siguiente:
  - La configuración de red y de seguridad del gabinete M1000e.
  - 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 los servidores.
  - Los controles de congruencia de la red Fabric de E/S entre los módulos de E/S y los servidores. Además, la CMC desactiva componentes, si es necesario, para proteger el hardware del sistema.
  - La seguridad de acceso de los usuarios.

Puede configurar el CMC para que envíe correos electrónicos o alertas de capturas SNMP por advertencias o errores relacionados con temperatura, configuración errónea del hardware, interrupciones de alimentación y velocidad del ventilador.

Temas:

- Cómo ponerse en contacto con Dell

Novedades de esta versión

Esta versión de la CMC para Dell PowerEdge M1000e ofrece:

- Visualización de la velocidad de los ventiladores e información de la temperatura mediante WSMan.
- Demonio de código abierto LLDP para reenviar los paquetes LLDP a la iDRAC mediante VLAN.
- Transferencia de dumplogs de la CMC a la iDRAC.

Funciones clave

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

Funciones de administración

El CMC proporciona las siguientes funciones de administración:

- Entorno redundante del CMC.
- Registro del sistema dinámico de nombres de dominio (DDNS) para IPv4 e IPv6.
- Administración y supervisión remotas del sistema por medio de SNMP, una interfaz web, iKVM o una conexión de Telnet o SSH.
- Supervisión: proporciona acceso a la información del sistema y al estado de los componentes.
- Acceso a registros de sucesos del sistema: proporciona acceso al registro de hardware y al registro del CMC.
- Actualizaciones de firmware para diversos componentes del chasis: permite actualizar el firmware para CMC, servidores, iKVM y dispositivos de infraestructura de módulo de E/S.
- Actualización de firmware para componentes del servidor, como el BIOS, las controladoras de red o las controladoras de almacenamiento, en varios servidores del chasis con Lifecycle Controller.
- Actualización de componentes del servidor: permite usar un solo clic para todas las actualizaciones blade mediante el modo Actualizar desde recurso compartido de red.
- Integración con el software Dell OpenManage: permite iniciar la interfaz web del CMC desde Dell OpenManage Server Administrator o IT Assistant.
- Alerta del CMC: alerta sobre problemas potenciales del nodo administrado mediante un mensaje por correo electrónico o una captura SNMP.
- Administración remota de la alimentación: proporciona funciones remotas de administración de la alimentación, como el apagado y el restablecimiento de cualquier componente del chasis, desde una consola de administración.
- Informe de uso de la alimentación.
- Cifrado de capa de sockets seguros (SSL): ofrece administración remota y segura de sistemas mediante la interfaz web.
- Punto de inicio para la interfaz web de Integrated Dell Remote Access Controller (iDRAC).
- Compatibilidad con WS-Management.
- Función FlexAddress: reemplaza las 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.
- Compatibilidad de la función de identidad de E/S del iDRAC con el inventario mejorado de direcciones WWN/MAC.
- Gráfico de la condición y el estado de los componentes del chasis.
- Asistencia para servidores simples o de varias ranuras.
- Compatibilidad del asistente de configuración iDRAC con LCD con la configuración de la red del iDRAC.
- Inicio de sesión único de iDRAC.
- Compatibilidad para el protocolo de hora de red (NTP).
- Resumen de servidores, informe de la alimentación y páginas de control de la alimentación mejorados.
- Protección forzada contra fallas del CMC y recolocación virtual de servidores.
- Restablecimiento del iDRAC sin reiniciar el sistema operativo.
- Compatibilidad con configuración de arreglo de almacenamiento mediante RACADM: Le permite configurar IP, sumarse a grupos o crearlos, y seleccionar red Fabric para arreglos de almacenamiento mediante RACADM.
- Administración de múltiples chasis:
  - capacidad de visualizar hasta ocho chasis miembro de grupo desde el chasis principal.
  - capacidad de seleccionar las propiedades de configuración del Chasis principal y aplicarlas en los miembros de grupo.
  - capacidad para que los miembros del grupo mantengan la configuración de su chasis sincronizada con el chasis principal.

- Compatibilidad para guardar la información de configuración y las opciones de los servidores en el disco duro para restaurar al mismo servidor o a uno diferente.

Funciones de seguridad

El 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 donde se usa un esquema estándar o un esquema extendido (opcional).
  - Identificaciones y contraseñas de usuarios guardadas en el hardware.
- Autoridad basada en funciones: permite que el administrador configure privilegios específicos para cada usuario.
- Configuración de identificaciones y contraseñas de usuario por medio de la interfaz web.

  NOTA: 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 que pueden configurarse (si corresponde)
- Límites de errores de inicio de sesión por dirección IP, con bloqueo de inicio de sesión proveniente de la dirección IP cuando esta última ha superado el límite.
- Límite de tiempo de espera de sesión automático y configurable, y varias sesiones simultáneas.
- Rango limitado de direcciones IP para clientes que se conectan a la CMC.
- Secure Shell (SSH), que utiliza una capa cifrada para ofrecer una mayor seguridad.
- Inicio de sesión único, autentificación de dos factores y autentificación de clave pública.

Descripción general del chasis

En la ilustración siguiente se muestra el borde frontal de un CMC (interior) y las ubicaciones de las ranuras del CMC en el chasis.

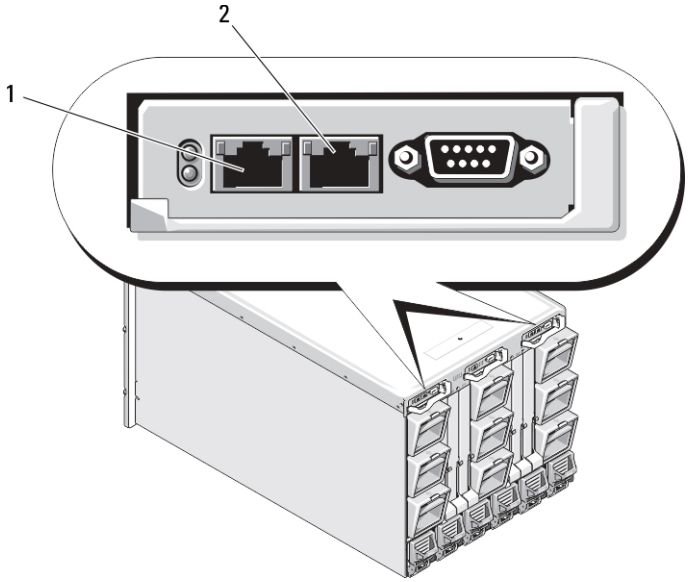


Ilustración 1. Ubicación de las ranuras de la CMC en el chasis

Tabla 1. Detalles de la ubicación de las ranuras de la CMC

1	Puerto GB
2	Puerto STK

Información de puertos del CMC

Se requieren los siguientes puertos TCP/IP para obtener acceso remoto a CMC con servidores de seguridad. Son los puertos que la CMC utiliza para detectar las conexiones.

Tabla 2. Puertos de detección de servidores del CMC

Número de puerto	Función
22*	SSH
23*	Telnet
80*	HTTP
161	Agente SNMP
443*	HTTPS

* Puerto configurable

En la tabla siguiente se enumeran los puertos que el CMC utiliza como cliente.

Tabla 3. Puerto cliente del CMC

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

* Puerto configurable

Versión mínima de CMC

En la siguiente tabla se incluye la versión mínima de CMC que se requiere para activar los servidores blade enumerados.

Tabla 4. Versión de CMC mínima para los servidores blade

Servidores	Versión mínima de CMC
PowerEdge M600	CMC 1.0
PowerEdge M605	CMC 1.0
PowerEdge M805	CMC 1.2
PowerEdge M905	CMC 1.2
PowerEdge M610	CMC 2.0
PowerEdge M610x	CMC 3.0
PowerEdge M710	CMC 2.0
PowerEdge M710hd	CMC 3.0
PowerEdge M910	CMC 2.3

Tabla 4. Versión de CMC mínima para los servidores blade (continuación)

Servidores	Versión mínima de CMC
PowerEdge M915	CMC 3.2
PowerEdge M420	CMC 4.1
PowerEdge M520	CMC 4.0
PowerEdge M620	CMC 4.0
PowerEdge M820	CMC 4.11
PowerEdge PSM4110	CMC 4.11
PowerEdge M630	CMC 5.0
PowerEdge M830	CMC 5.0
PowerEdge M640	CMC 6.0

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

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

Conmutadores de módulo de E/S	Versión mínima de CMC
PowerConnect M6220	CMC 1.0
PowerConnect M6348	CMC 2.1
PowerConnect M8024	CMC 1.2
PowerConnect M8024-k	CMC 3.2
PowerConnect M8428-k	CMC 3.1
Módulo de paso a través 10/100/1000Mb Ethernet de Dell	CMC 1.0
Módulo de paso FC de 4 Gbps de Dell	CMC 1.0
Módulo SAN FC de 8/4 Gbps de Dell	CMC 1.2
Módulo de paso a través 10Gb Ethernet de Dell	CMC 2.1
Módulo II de paso a través 10Gb Ethernet de Dell	CMC 3.0
Módulo de paso a través de K 10Gb Ethernet de Dell	CMC 3.0
Brocade M4424	CMC 1.0
Brocade M5424	CMC 1.2
Cisco Catalyst CBS 3130X-S	CMC 1.0
Cisco Catalyst CBS 3130G	CMC 1.0
Cisco Catalyst CBS 3032	CMC 1.0
Dell Force10 MXL 10/40GbE	CMC 4.11
Conmutador de agregación de E/S Dell PowerEdge M	CMC 4.2
Conmutador Infiniband DDR Mellanox M2401G	CMC 1.0
Conmutador Infiniband QDR Mellanox M3601Q	CMC 2.0
Conmutador Infiniband FDR/QDR Mellanox M4001F/M4001Q	CMC 4.0
Conmutador Infiniband FDR10 Mellanox M4001T	CMC 4.1
Brocade M6505	CMC 4.3
Cisco Nexus B22DELL	CMC 4.3

Versiones de firmware más recientes de esta publicación

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

Tabla 6. Versiones de firmware más recientes de BIOS, iDRAC y Lifecycle Controller

Servidores	BIOS	iDRAC	Lifecycle Controller
PowerEdge M600	2.4.0	1.65	No aplicable
PowerEdge M605	5.4.1	1.65	No aplicable
PowerEdge M805	2.3.3	1.65	No aplicable
PowerEdge M905	2.3.3	1.65	No aplicable
PowerEdge M610	6.3.0	3.50	1,6
PowerEdge M610x	6.3.0	3.50	1,6
PowerEdge M710	6.4.0	3.80	1.7.5.4
PowerEdge M710hd	7.0.0	3.50	1,6
PowerEdge M910	2.9.0	3.50	1,6
Power Edge M915	3.2.2	3.80	1.7.5.4
PowerEdge M420	2.3.3	2.40.40.40	2.40.40.40
PowerEdge M520	2.4.2	2.40.40.40	2.40.40.40
PowerEdge M620	2.5.4	2.40.40.40	2.40.40.40
PowerEdge M820	2.3.3	2.40.40.40	2.40.40.40
PowerEdge M630	2.2.5	2.40.40.40	2.40.40.40
PowerEdge M830	2.2.5	2.40.40.40	2.40.40.40
PowerEdge M640	1.0.0	3.10.10.10	3.10.10.10

NOTA: El software de la matriz versión 6.0.4 es compatible con PowerEdge PSM4110.

Conexiones de acceso remoto admitidas

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

Tabla 7. Conexiones de acceso remoto admitidas

Conexión	Características
Puertos de la interfaz de red de la CMC	• Puerto GB: Interfaz de red exclusiva para la interfaz web de la CMC. Dos puertos de 10/100/1000 Mbps, uno para administración y otro para consolidación de cables entre chasis. • STK: puerto de enlace ascendente para la consolidación de cables entre chasis de la red de administración. • Ethernet de 10 Mbps/100 Mbps/1 Gbps a través de puerto GbE del CMC. • Compatibilidad con DHCP. • Capturas SNMP y notificación de sucesos por correo electrónico. • 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.

Tabla 7. Conexiones de acceso remoto admitidas (continuación)

Conexión	Características
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 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).
Otras conexiones	• Acceso a Dell CMC Console por medio del módulo de conmutador KVM integrado Avocent (iKVM).

Plataformas admitidas

La CMC admite sistemas modulares diseñados para la plataforma PowerEdge M1000e. Para obtener información sobre la compatibilidad con la CMC, consulte la documentación de su dispositivo.

Para conocer las plataformas compatibles más recientes, consulte *Chassis Management Controller Version 6.0 Release Notes (Notas de publicación de Chassis Management Controller versión 6.0)*, disponible en **dell.com/cmcmanuals**.

Exploradores web admitidos para la estación de administración

Para obtener la información más reciente sobre los navegadores web admitidos, consulte *Chassis Management Controller Version 6.0 Release Notes (Notas de publicación de Chassis Management Controller versión 6.0)*, disponible en **dell.com/cmcmanuals**.

- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari versión 7
- Safari versión 8
- Safari versión 9
- Mozilla Firefox 52
- Mozilla Firefox 53
- Google Chrome 57
- Google Chrome 58

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+
```

Visualización de versiones traducidas de la interfaz web del CMC

Para ver las versiones traducidas de la interfaz web del CMC:

1. Abra **Control Panel (Panel de control)** en Windows.
2. Haga doble clic en el icono **Opciones regionales**.

3. Seleccione la opción regional necesaria en el menú desplegable **Configuración regional (ubicación)**.

Aplicaciones admitidas de la consola de administración

La CMC admite la integración con Dell OpenManage IT Assistant. Para obtener más información, consulte la documentación de IT Assistant disponible en el sitio web de asistencia de Dell **dell.com/support/manuals**.

Otros documentos que podrían ser de utilidad

Además de esta guía, puede acceder a las siguientes guías disponibles en **dell.com/support/manuals**. Seleccione **Choose from a list of all Dell products (Elegir de una lista de todos los productos Dell)** y haga clic en **Continue (Continuar)**. Haga clic en **Software, Monitors, Electronics & Peripherals (Software, monitores, dispositivos electrónicos y periféricos)** > **Software**:

- Haga clic en **Remote Enterprise System Management (System Management de Remote Enterprise)** y, a continuación, en **Dell Chassis Management Controller Version 6.0 (Dell Chassis Management Controller versión 6.0)** para ver:
  - En *CMC Online Help (Ayuda en línea para el CMC)*, se proporciona información sobre el uso de la interfaz web.
  - En *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* (Especificaciones técnicas de la tarjeta Secure Digital [SD] de Chassis Management Controller [CMC]), se proporciona información sobre el uso, la instalación y la versión mínima de firmware y de BIOS.
  - La publicación *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) acerca de los subcomandos de RACADM, las interfaces admitidas y los grupos de base de datos de propiedades y las definiciones de objetos.
  - *Chassis Management Controller Version 6.0 Release Notes (Notas de publicación de Chassis Management Controller versión 6.0)*, disponible en **dell.com/cmcmanuals**, ofrece actualizaciones de último momento relativas al sistema, documentación o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- Haga clic en **Remote Enterprise System Management** (System Management de Remote Enterprise) y luego haga clic en el número de versión necesario del iDRAC para ver la publicación *Integrated Dell Remote Access Controller (iDRAC) User's Guide* (Guía del usuario de Integrated Dell Remote Access Controller (iDRAC) que proporciona información sobre la instalación, la configuración y el mantenimiento del iDRAC en sistemas administrados.
- Haga clic en **Enterprise System Management (System Management de Enterprise)** y luego haga clic en el nombre del producto para ver los siguientes documentos:
  - 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.

Los siguientes documentos del sistema disponibles en **dell.com/support/manuals** proporcionan más información sobre el sistema que el CMC está instalado:

- 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 las guías *Rack Installation Guide (Guía de instalación en bastidor)* y *Rack Installation Instructions (Instrucciones de instalación en bastidor)* que se incluyen con el bastidor, se describe la forma de instalar el sistema en un bastidor.
- En *Hardware Owner's Manual (Manual del propietario de hardware)*, se proporciona información acerca de las funciones del sistema y se describe la forma de solucionar problemas en el sistema e instalar o sustituir componentes.
- 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.
- Es posible que se incluyan archivos Léame o notas de la versión 6.0 de Chassis Management Controller para ofrecer actualizaciones de último momento relativas al sistema, documentación o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- Para obtener más información sobre la configuración de red del módulo de E/S, consulte el documento *Dell PowerConnect M6220 Switch Important Information (Información importante sobre el conmutador Dell PowerConnect M6220)* y el documento técnico *Dell PowerConnect 6220 Series Port Aggregator White Paper (Documento técnico sobre el agregador de puertos Dell PowerConnect serie 6220)*.
- Documentación específica para la aplicación de consola de administración de otros fabricantes.

Acceso a contenido de soporte desde el sitio de soporte de Dell EMC

Acceda al contenido de soporte relacionado con un arreglo de herramientas de administración de sistemas mediante enlaces directos, vaya al sitio de soporte de Dell EMC o use un motor de búsqueda.

- Enlaces directos:
  - Para Dell EMC Enterprise Systems Management y Dell EMC Remote Enterprise Systems Management:https://www.dell.com/esmmanuals
  - Para Dell EMC Virtualization Solutions:https://www.dell.com/SoftwareManuals
  - Para Dell EMC OpenManage:https://www.dell.com/openmanagemanuals
  - Para iDRAC:https://www.dell.com/idracmanuals
  - Para Dell EMC OpenManage Connections Enterprise Systems Management:https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Para Dell EMC Serviceability Tools:https://www.dell.com/serviceabilitytools
- Sitio de soporte de Dell EMC:
  1. Vaya a https://www.dell.com/support.
  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 enlace necesario.
  4. Haga clic en el producto necesario y, luego, haga clic en la versión necesaria.

Mediante los motores de búsqueda, escriba el nombre y la versión del documento en el cuadro Buscar.

Cómo ponerse en contacto con Dell

NOTA: Si no tiene una conexión a Internet activa, puede encontrar información de contacto en su factura de compra, en su albarán de entrega, en su recibo o en el catálogo de productos Dell.

Dell proporciona varias opciones de servicio y asistencia en línea y por teléfono. La disponibilidad varía según el país y el producto y es posible que algunos de los servicios no estén disponibles en su área. Si desea ponerse en contacto con Dell para tratar cuestiones relacionadas con las ventas, la asistencia técnica o el servicio de atención al cliente:

1. Vaya a **Dell.com/support.**
2. Seleccione la categoría de soporte.
3. Seleccione su país o región en la lista desplegable **Elija un país o región** que aparece al final de la página.
4. Seleccione el enlace de servicio o asistencia apropiado en función de sus necesidades.

2

Instalación y configuración del CMC

En esta sección se proporciona información acerca de la forma de instalar el hardware de Chassis Management Controller (CMC) PowerEdge M1000e, establecer el acceso al CMC, configurar el entorno de administración para utilizar el CMC, y usar los siguientes pasos como guía para configurar el CMC:

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

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

Temas:

Antes de empezar

Antes de configurar el entorno del CMC, descargue la versión más reciente del firmware del CMC de **support.dell.com**.

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

Instalación de hardware del CMC

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

Conceptos relacionados

Descripción del entorno de CMC redundante en la página 36

Lista de comprobación para configurar el chasis

Los siguientes pasos permiten configurar el chasis con precisión:

1. Asegúrese de que la CMC y la estación de administración donde utiliza el navegador estén en la misma red, que se denomina red de administración. Conecte un cable de red Ethernet del puerto **GB** de la CMC a la red de administración.

   NOTA: No coloque ningún cable en el puerto Ethernet **STK** de la CMC. Para obtener más información sobre el cable para el puerto STK, consulte Descripción del entorno de CMC redundante.
2. Instale los módulos de E/S en el chasis y conecte los cables.

3. Inserte los servidores en el chasis.
4. Conecte el chasis a la fuente de alimentación.
5. Presione el botón de encendido ubicado en la esquina inferior izquierda del chasis o encienda el chasis desde la interfaz web del CMC después de completar el paso 7.

   NOTA: No encienda los servidores.
6. Por medio del panel LCD que se encuentra en el área frontal del sistema, proporcione una dirección IP estática al CMC o configure el CMC para DHCP.
7. Conéctese a la dirección IP del CMC y proporcione un nombre de usuario predeterminado (root) y una contraseña (calvin).
8. Proporcione una dirección IP a cada iDRAC en la interfaz web del CMC y active la interfaz LAN e IPMI.

   NOTA: La interfaz LAN del iDRAC está desactivada en algunos servidores de forma predeterminada.
9. Proporcione una dirección IP a cada módulo de E/S en la interfaz web del CMC.
10. Conéctese a cada iDRAC y realice la configuración final de la iDRAC. El nombre de usuario predeterminado es *root* y la contraseña es *calvin.*
11. Conéctese a cada módulo de E/S a través del explorador web y lleve a cabo la configuración final del módulo de E/S.
12. Encienda los servidores e instale el sistema operativo.

Conexión básica del CMC a la red

PRECAUCIÓN: La conexión del puerto STK a la red de administración puede ocasionar resultados imprevisibles. La conexión de los puertos GB y STK a la misma red (dominio de transmisión) puede causar una tormenta de difusión.

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

Cada CMC tiene dos puertos Ethernet RJ-45 marcados como **GB** (el puerto de enlace ascendente) y **STK** (el puerto de consolidación de cable o apilamiento). Con cableado básico, puede conectar el puerto GB a la red de administración y no utilizar el puerto STK.

Conexión en cadena tipo margarita del CMC a la red

Si tiene varios chasis en un bastidor, puede reducir el número de conexiones a la red de administración mediante la conexión en cadena de hasta cuatro chasis entre sí. Si cada uno de estos cuatro chasis contiene una CMC redundante, la conexión en cadena tipo margarita permite reducir de ocho a dos el número de conexiones a la red de administración. Si cada chasis solo tiene una CMC, el número de conexiones necesarias se puede reducir de cuatro a una.

Cuando los chasis se conectan en cadena tipo 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 el chasis que esté más cerca de la red. El puerto STK se debe conectar solamente a un puerto GB más alejado de la cadena o la red.

Cree cadenas separadas para los CMC en la ranura del CMC activo y en la segunda ranura del CMC.

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

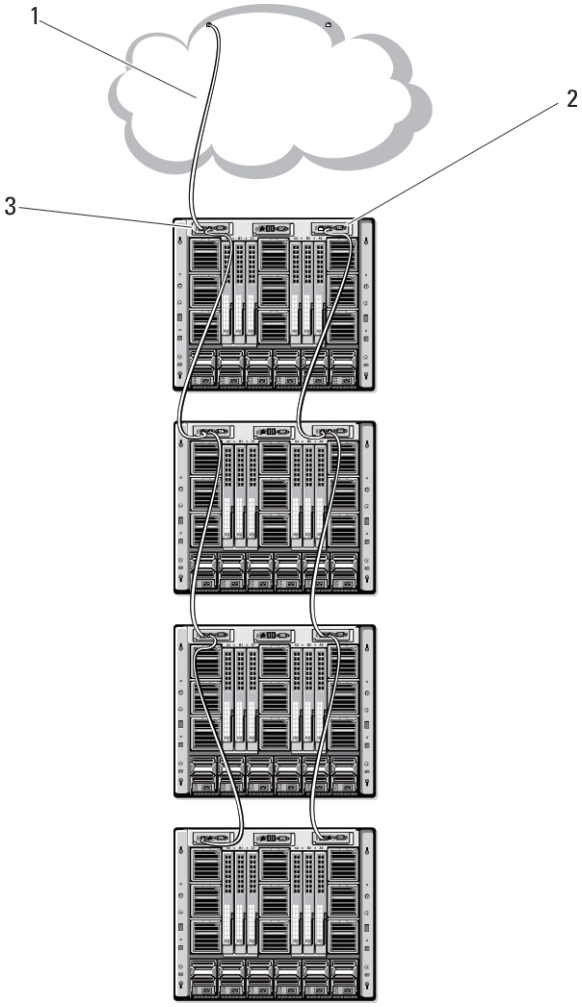


Ilustración 2. Conexión en cadena tipo margarita de la CMC a la red

1	Red de administración
2	CMC en espera
3	CMC activa

En las siguientes figuras se proporcionan ejemplos de cableado incorrecto en el CMC.

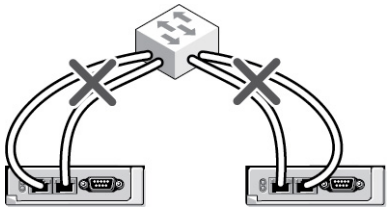


Ilustración 3. Cableado incorrecto para la red de la CMC: 2 CMC

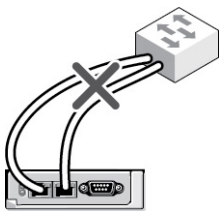


Ilustración 4. Cableado incorrecto para la red de la CMC: CMC único

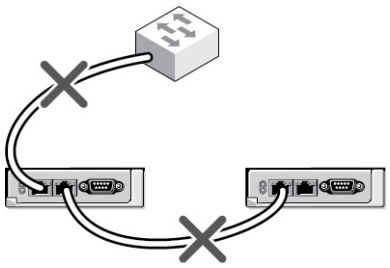


Ilustración 5. Cableado incorrecto para la red de la CMC: 2 CMC

Para conectar hasta cuatro chasis en cadena tipo margarita:

1. Conecte a la red de administración el puerto GB del CMC activo en el primer chasis.
2. Conecte el puerto GB del CMC activo en el segundo chasis al puerto STK del CMC activo en el primer chasis.
3. Si existe un tercer chasis, conecte el puerto GB del CMC activo al puerto STK del CMC activo en el segundo chasis.
4. Si existe un cuarto chasis, conecte el puerto GB del CMC activo al puerto STK del tercer chasis.
5. Si existen CMC redundantes en el chasis, conéctelos utilizando el mismo patrón.

   PRECAUCIÓN: El puerto STK de cualquier CMC no se debe conectar nunca 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 generar interrupciones en la red y provocar la pérdida de datos. La conexión de los puertos GB y STK a la misma red (dominio de transmisión) puede causar una tormenta de difusión.

   NOTA: No conecte un CMC activo a un CMC en espera.

   NOTA: El restablecimiento de una CMC cuyo puerto STK está conectado en cadena a otra CMC puede generar interrupciones en la red para las CMC que aparecen más adelante en la cadena. Las CMC subordinadas podrían registrar mensajes que indiquen que se ha perdido la conexión con la red, y podrían desactivarse y ceder sus funciones a las CMC redundantes.
6. Para comenzar a usar el CMC, consulte Installing Remote Access Software on a Management Station (Instalación de software de acceso remoto en una estación de administración).

Instalación de software de acceso remoto en una estación de administración

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

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

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

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

Instalación de RACADM en una estación de administración con Linux

1. Inicie sesión como usuario raíz en el sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE Linux Enterprise Server admitido en el que desea instalar los componentes de Managed System.
2. Inserte el DVD *Dell Systems Management Tools and Documentation (Documentación y herramientas de Dell Systems Management)* en la unidad de DVD.
3. Para montar el DVD en una ubicación requerida, utilice el comando mount o un comando similar.

NOTA: En el sistema operativo Red Hat Enterprise Linux 5, los DVD se montan automáticamente con la opción `-noexec mount`. Esta opción no le permite iniciar ningún archivo ejecutable desde el DVD. Debe montar el DVD-ROM manualmente y luego iniciar los ejecutables.

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 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

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

Desinstalación de RACADM desde una estación de administración con Linux

1. Inicie sesión como root en el sistema en el que desea instalar los componentes 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 command`

Configuración de un explorador web

Puede configurar y administrar la CMC, los servidores y los módulos instalados en el chasis mediante un navegador web. Consulte la sección *Supported Browsers (Navegadores admitidos)* en el archivo *Readme (Léame),* disponible 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*. En función de los requisitos de seguridad, la red de administración puede ser una red aislada muy 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 al CMC.

Algunas funciones de los exploradores pueden interferir con la conectividad o el rendimiento, especialmente si la red de administración no tiene una ruta a Internet. Si la estación de administración ejecuta un sistema operativo Windows, algunas configuraciones de Internet Explorer pueden interferir con la conectividad, incluso cuando se utiliza una interfaz de línea de comandos para obtener acceso a la red de administración.

Conceptos relacionados

Servidor proxy en la página 26

Tareas relacionadas

Filtro de suplantación de identidad de Microsoft en la página 27
Obtención de la lista de revocación de certificados en la página 27
Descarga de archivos desde el CMC con Internet Explorer en la página 27
Activación de animaciones en Internet Explorer en la página 28

Servidor proxy

Para explorar a través de 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 navegador. Esto indica al navegador que pase por alto el servidor proxy al acceder a la red de administración.

Internet Explorer

Para editar la lista de excepciones en Internet Explorer:

1. Inicie Internet Explorer.
2. Haga clic en **Herramientas** > **Opciones de Internet** > **Conexiones**.
3. En la sección **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.
   Aparecerá el cuadro de diálogo **Configuración de la red de área local (LAN)**.
4. En el cuadro de diálogo **Local Area Network (LAN) settings (Configuración de la red de área local, LAN)**, vaya a la sección **Proxy server (Servidor proxy)**. Seleccione la opción **Use a proxy server for your LAN (Usar un servidor proxy para la LAN)**.
   Se activará la opción **Avanzado**.
5. Haga clic en **Advanced (Opciones avanzadas)**.
6. En la sección **Exceptions (Excepciones)**, agregue las direcciones para las CMC y las iDRAC en la red de administración mediante una lista de valores separados por punto y coma. Puede usar nombres DNS y comodines en las entradas.

Mozilla Firefox

Para editar la lista de excepciones en Mozilla Firefox versión 3.0:

1. Abra Mozilla Firefox.
2. Haga clic en **Herramientas** > **Opciones** (para sistemas que ejecutan Windows) o haga clic en **Editar** > **Preferencias**(para sistemas que ejecutan Linux).
3. Haga clic en **Avanzado** y luego en la ficha **Red**.
4. Haga clic en **Configuración**.
5. Seleccione la opción **Configuración manual del proxy**.
6. En el campo **No Proxy for (No usar proxy para)**, escriba una lista con las direcciones para las CMC y las iDRAC de la red de administración separadas por comas. Puede usar nombres DNS y comodines en las entradas.

Filtro de suplantación de identidad de Microsoft

Si se activa el filtro de suplantación de identidad de Microsoft en Internet Explorer 7 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 navegador u otra interfaz como RACADM remoto. Siga estos pasos 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. Active la casilla **Desactivar el filtro de suplantación de identidad** y haga clic en **Aceptar**.

Obtención de la lista de revocación de certificados

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

Para desactivar la obtención de la CRL:

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

Descarga de archivos desde el CMC con Internet Explorer

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

Para activar la opción **Do not save encrypted pages (No guardar las páginas cifradas en el disco)**:

1. Inicie Internet Explorer.
2. Haga clic en **Herramientas** > **Opciones de Internet** > **Avanzado**.
3. Desplácese a la sección **Seguridad** y seleccione **No guardar las páginas cifradas en el disco**.

Activación de animaciones en Internet Explorer

Al transferir archivos hacia y desde la interfaz web, el icono de transferencia de archivos gira para indicar la actividad de transferencia. Si usa Internet Explorer, debe configurar el navegador para que reproduzca animaciones.

Para configurar Internet Explorer para reproducir animaciones:

1. Inicie Internet Explorer.
2. Haga clic en **Herramientas** > **Opciones de Internet** > **Avanzado**.
3. Desplácese a la sección **Multimedia** y seleccione la opción **Activar animaciones en páginas web**.

Configuración del acceso inicial al CMC

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

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

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

Asegúrese de que la CMC y la iDRAC de cada servidor y los puertos de administración de red de todos los módulos de E/S del conmutador se conecten a una red interna común en el chasis M1000e. Esto permite aislar la red de administración de la red de datos de servidores. Es importante separar el tráfico para garantizar el acceso ininterrumpido a las funciones de administración del chasis.

La CMC se conecta a la red de administración. Todo el acceso externo a la CMC y a las iDRAC se realiza mediante la CMC. El acceso a los servidores administrados, en cambio, se obtiene mediante conexiones de red a módulos de E/S (IOM). Esto permite aislar la red de aplicaciones de la red de administración.

Se recomienda aislar la administración del chasis de la red de datos. Dell no puede ofrecer ni garantizar tiempo de actividad en un chasis que no se ha integrado correctamente al entorno. 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 de la CMC y la iDRAC. Estas demoras pueden provocar un comportamiento impredecible en el chasis; por ejemplo, que la CMC indique que la iDRAC está fuera de línea aunque esté encendida 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 la iDRAC a una red VLAN aparte. Las interfaces de red de la CMC y de cada iDRAC pueden configurarse para que utilicen una VLAN.

Si tiene un chasis, conecte la CMC y la CMC en espera a la red de administración. Si tiene una CMC redundante, utilice otro cable de red y conecte el puerto **GB** de la CMC a un segundo puerto de la red de administración.

Si tiene más de un chasis, puede elegir entre la conexión básica, donde cada CMC está conectada a la red de administración, o una conexión de chasis en cadena margarita, donde los chasis están conectados en serie y solo una CMC se conecta a la red de administración. El tipo de conexión básica utiliza más puertos en la red de administración y proporciona mayor redundancia. El tipo de conexión en cadena margarita utiliza menos puertos en la red de administración, pero introduce dependencias entre las CMC, lo cual reduce la redundancia del sistema.

NOTA: Si el CMC no se conecta de forma adecuada en una configuración redundante, existe la posibilidad de que se pierda el acceso a la administración y se creen tormentas de difusión.

Conceptos relacionados

Conexión básica del CMC a la red en la página 23
Conexión en cadena tipo margarita del CMC a la red en la página 23
Configuración inicial de red del CMC en la página 28

Configuración inicial de red del CMC

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

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

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

Para configurar las opciones iniciales de red después de asignar una dirección IP al CMC, se puede utilizar cualquiera de las siguientes interfaces:

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

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

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

NOTA: La opción de configurar la CMC mediante el panel LCD solo se encuentra disponible hasta que se implementa la CMC o se cambia la contraseña predeterminada. Si no se cambia la contraseña, puede seguir usando el LCD para restablecer las configuraciones de la CMC, lo cual constituye un posible riesgo para la seguridad.

El panel LCD se encuentra en la esquina inferior izquierda en la parte delantera del chasis.

Para configurar una red mediante la interfaz del panel LCD:

1. Presione el botón de encendido del chasis para encenderlo.

   La pantalla LCD muestra una serie de pantallas de inicialización al encenderse. Cuando está lista, aparece la pantalla **Language Setup (Configuración de idioma)**.

2. Seleccione el idioma con los botones de flecha. A continuación, presione el botón central para seleccionar **Aceptar/Sí** y presione nuevamente el botón central.

   La pantalla **Gabinete** muestra la siguiente pregunta: **¿Configurar gabinete?**

   - Presione el botón central para avanzar a la pantalla **Configuración de red del CMC**. Consulte el paso 4.
   - Para salir del menú **Configure Enclosure (Configurar gabinete)**, seleccione el icono NO y presione el botón central. Consulte el paso 9.

3. Presione el botón central para avanzar a la pantalla **Configuración de red del CMC**.
4. Seleccione la velocidad de la red (10 Mbps, 100 Mbps, Automática [1 Gbps]) con el botón de flecha hacia abajo.

   El valor de Velocidad de la red debe coincidir con la configuración de la red para obtener un rendimiento de red efectivo. Un valor de Velocidad de la red inferior a la velocidad en la configuración de la red aumenta el consumo de ancho de banda y reduce la velocidad de la comunicación de red. **Determine si la red admite las velocidades de red mencionadas y seleccione la velocidad que corresponda**. Si la configuración de la red no coincide con alguno de estos valores, se recomienda utilizar negociación automática (la opción **Auto [Automática]**) o consultar al fabricante de los equipos de red.

   Presione el botón central para avanzar a la siguiente pantalla de **Configuración de red del CMC**.

5. Seleccione el modo dúplex (medio o completo) que corresponda al entorno de red.

   NOTA: La configuración de la velocidad de la red y de modo dúplex no estará disponible si Negociación automática se establece como Activada o si se selecciona 1000 MB (1 Gbps).

   Si la negociación automática se activa para un dispositivo pero no para el otro, el dispositivo que utiliza la negociación automática puede determinar la velocidad de la red del otro dispositivo, pero no el modo dúplex; en este caso, el modo dúplex toma el valor predeterminado de dúplex medio durante la negociación automática. Una incompatibilidad de dúplex de este tipo genera una conexión de red lenta.

   Presione el botón central para avanzar a la siguiente pantalla de **Configuración de red del CMC**.

6. Seleccione el protocolo de Internet (IPv4, IPv6 o ambos) que desea usar para el CMC y presione el botón central para avanzar a la siguiente pantalla de **Configuración de red del CMC**.
7. Seleccione el modo en el que desea que el CMC obtenga las direcciones IP de NIC:

Protocolo de configuración dinámica de host (DHCP)	La CMC recupera automáticamente la configuración de IP (dirección IP, máscara y puerta de enlace) de un servidor DHCP en la red. La CMC tiene una dirección IP exclusiva asignada en la red. Si ha seleccionado la opción DHCP, presione el botón central. Aparecerá la pantalla **Configure iDRAC (Configurar iDRAC)**; vaya al paso 9.

Estática

La dirección IP, la puerta de enlace y la máscara de subred en las pantallas que siguen inmediatamente se introducen de forma manual.

Si seleccionó la opción **Estática**, presione el botón central para avanzar a la siguiente pantalla de **Configuración de red del CMC**. A continuación:

- Defina el valor de **Static IP Address (Dirección IP estática)** usando las teclas de flecha hacia la derecha o la izquierda para desplazarse por las posiciones, y las teclas de flecha hacia arriba y abajo para seleccionar un número en cada posición. Cuando haya terminado de configurar el valor de **Static IP Address (Dirección IP estática)**, presione el botón central para continuar.
- Establezca la máscara de subred y, a continuación, presione el botón central.
- Establezca la puerta de enlace y, a continuación, presione el botón central. Aparecerá la pantalla **Network Summary (Resumen de red)**.

  En la pantalla **Network Summary (Resumen de red)** se presentan los valores introducidos para las opciones **Static IP Address (Dirección IP estática)**, **Subnet Mask (Máscara de subred)** y **Gateway (Puerta de enlace)**. Verifique que los valores sean los correctos. Para corregir un valor, vaya al botón de flecha hacia la izquierda y presione la tecla central para regresar a la pantalla del valor. Después de hacer la corrección, presione el botón central.

- Cuando esté satisfecho con todos los valores, presione el botón central. Aparecerá la pantalla **Register DNS? (¿Registrar DNS?)** .

NOTA: Si se selecciona el modo de protocolo de configuración dinámica de host (DHCP) para la configuración de IP del CMC, el registro de DNS también se activa de manera predeterminada.

8. Si seleccionó **DHCP** en el paso anterior, vaya al paso 10.

   Si desea registrar la dirección IP del servidor DNS, presione el botón central para continuar. Si no tiene DNS, presione la tecla de flecha hacia la derecha. Aparecerá la pantalla **Register DNS? (¿Registrar DNS?)** ; vaya al paso 10.

   Defina el valor de **DNS IP Address (Dirección IP de DNS)** usando las teclas de flecha hacia la derecha o la izquierda para desplazarse por las posiciones, y las teclas de flecha hacia arriba y abajo para seleccionar un número en cada posición. Cuando haya terminado de configurar la dirección IP de DNS, presione el botón central para continuar.

9. Indique si desea configurar el iDRAC:
   - **No**: vaya al paso 13.
   - **Sí**: presione el botón central para continuar.

   También puede configurar el iDRAC desde la interfaz gráfica de usuario del CMC.

10. Seleccione el protocolo de Internet (IPv4, IPv6 o ambos) que desea usar para los servidores.

Protocolo de configuración dinámica de host (DHCP)

La iDRAC recupera automáticamente la configuración de IP (dirección IP, máscara y puerta de enlace) de un servidor DHCP en la red. La iDRAC tiene una dirección IP exclusiva asignada en la red. Presione el botón central.

Estática

En las pantallas que siguen inmediatamente, debe introducir de forma manual la dirección IP, la puerta de enlace y la máscara de subred.

Si seleccionó la opción **Estática**, presione el botón central para avanzar a la siguiente pantalla de **Configuración de red del iDRAC**. A continuación:

- Defina el valor de **Static IP Address (Dirección IP estática)** usando las teclas de flecha hacia la derecha o la izquierda para desplazarse por las posiciones, y las teclas de flecha hacia arriba y abajo para seleccionar un número en cada posición. Esta dirección es la IP estática de la iDRAC que se encuentra en la primera ranura. La dirección IP estática de cada iDRAC posterior se calculará como un incremento de número de la ranura de esta dirección IP. Cuando haya terminado de configurar el valor de **Static IP Address (Dirección IP estática)**, presione el botón central para continuar.
- Establezca la máscara de subred y, a continuación, presione el botón central.
- Establezca la puerta de enlace y, a continuación, presione el botón central.

- Seleccione la opción **Enable (Activar)** o **Disable (Desactivar)** para el canal LAN de IPMI. Presione el botón central para continuar.
- En la pantalla **iDRAC Configuration (Configuración de iDRAC)**, para aplicar toda la configuración de red de la iDRAC en los servidores instalados, seleccione el icono **Accept/Yes (Aceptar/Sí)** y presione el botón central. Para no aplicar la configuración de red de la iDRAC en los servidores instalados, seleccione el icono **No**, presione el botón central y continúe con el paso c.
- En la siguiente pantalla **iDRAC Configuration (Configuración de iDRAC)**, para aplicar toda la configuración de red de la iDRAC en los servidores recién instalados, seleccione el icono Accept/Yes (Aceptar/Sí) y presione el botón central; cuando se inserte un

servidor nuevo en el chasis, la pantalla LCD le preguntará al usuario si desea implementar automáticamente el servidor usando los valores/las políticas de red configurados previamente. Para no aplicar la configuración de red de la iDRAC en los servidores recién instalados, seleccione el icono **No** y presione el botón central; cuando se inserte un servidor nuevo en el chasis, no se configurarán los valores de red de la iDRAC.

11. En la pantalla **Enclosure (Gabinete)**, para aplicar todos los valores del gabinete, seleccione el icono **Accept/Yes (Aceptar/Sí)** y presione el botón central. Para no aplicar la configuración del gabinete, seleccione el icono **No** y presione el botón central.
12. En la pantalla **IP Summary (Resumen de IP)**, revise las direcciones IP definidas para asegurarse de que sean las correctas. Para corregir un valor, vaya al botón de flecha hacia la izquierda y presione la tecla central para regresar a la pantalla del valor. Después de hacer la corrección, presione el botón central. De ser necesario, vaya al botón de flecha hacia la derecha y presione la tecla central para regresar a la pantalla **IP Summary (Resumen de IP)**.

    Después de confirmar que los valores que introdujo sean los correctos, presione el botón central. El Asistente de configuración se cerrará y lo llevará de regreso a la pantalla **Main Menu (Menú principal)**.

    NOTA: Si seleccionó **Sí/Aceptar**, aparecerá una pantalla **Espere** antes de que se muestre la pantalla **Resumen de IP**.

    La CMC y las iDRAC ahora estarán disponibles en la red. Puede acceder a la CMC en la dirección IP asignada mediante la interfaz web o interfaces de línea de comandos, como una consola serie, Telnet y SSH.

    NOTA: Después de haber completado la configuración de la red a través del asistente de configuración de LCD, el asistente ya no estará disponible.

Interfaces y protocolos para obtener acceso al CMC

Una vez definida la configuración de red de la CMC, puede acceder de forma remota a la CMC mediante varias interfaces. En la siguiente tabla se presentan las interfaces que puede utilizar para acceder a la CMC de forma remota.

NOTA: Dado que no ofrece tanta seguridad como las otras interfaces, Telnet viene desactivada de manera predeterminada. Para activar Telnet, use la Web, ssh o RACADM remoto.

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

Tabla 8. Interfaces del CMC

Interfaz	Descripción
Interfaz web	Proporciona acceso remoto a la CMC mediante una interfaz gráfica de usuario. La interfaz web está incorporada en el firmware de la CMC, y se puede acceder a ella por medio de la interfaz de NIC desde un navegador web compatible en la estación de administración. Para obtener una lista de exploradores web admitidos, consulte la sección Exploradores admitidos en *Chassis Management Controller Version 5.0 Release Notes* (Notas de la versión de Chassis Management Controller versión 5.0) en **dell.com/support/manuals**.
Interfaz de línea de comandos de RACADM remoto	Use esta utilidad de línea de comandos para administrar el CMC y sus componentes. Puede usar el RACADM de firmware o el RACADM remoto: ● El RACADM remoto es una utilidad cliente que se ejecuta en una estación de administración. Utiliza la interfaz de red fuera de banda para ejecutar los comandos de RACADM en los sistemas administrados y el canal HTTPS. La opción `-r` ejecuta el comando RACADM en una red. ● Puede acceder al RACADM de firmware iniciando sesión en la CMC mediante SSH o Telnet. Puede ejecutar los comandos de RACADM de firmware sin especificar la IP, el nombre de usuario ni la contraseña de la CMC. Después de entrar en el símbolo del sistema de RACADM, puede ejecutar directamente los comandos sin el prefijo racadm.
Panel LCD del chasis	Use la pantalla LCD en el panel frontal para realizar lo siguiente: ● Ver alertas, la dirección IP o MAC del CMC y las cadenas programables del usuario. ● Configurar DHCP ● Configure los valores de dirección IP estática del CMC. ● Ver la dirección MAC del CMC para el CMC activo. ● Ver la Id. de VLAN del CMC agregada al final de la dirección IP del CMC si la VLAN ya está configurada.

Tabla 8. Interfaces del CMC (continuación)

Interfaz	Descripción
Telnet	Proporciona a la línea de comandos acceso 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. Al transmitir información confidencial, utilice la interfaz SSH.
SSH	Use SSH para ejecutar comandos RACADM. SSH proporciona las mismas capacidades que la consola Telnet, pero utiliza una capa de transporte cifrado para mayor seguridad. El servicio SSH está activado de forma predeterminada en el CMC y se puede desactivar.
WSMan	Los servicios remotos LC se basan en el protocolo WS-Management para realizar tareas de administración de uno a varios sistemas. Debe utilizar un cliente WSMan, como el cliente WinRM (Windows) o el cliente Open WSMan (Linux), para utilizar la funcionalidad LC Remote Services. También puede utilizar Power Shell y Python para crear secuencias de comandos para la interfaz WSMan. Web Services for Management (WS-Management) 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 de WSMan de la CMC usa SSL en el puerto 443 para la seguridad del transporte y admite autentificación básica. Los datos disponibles a través de WS-Management se proporcionan con la interfaz de instrumentación del CMC asignada a los perfiles de DMTF y los perfiles de extensión. Para obtener más información, consulte lo siguiente: ● MOF y perfiles: **delltechcenter.com/page/DCIM.Library** ● Sitio web de DTMF: **dmtf.org/standards/profiles/** ● Notas de publicación o archivo Léame de WSMan. ● **www.wbemsolutions.com/ws_management.html** ● Especificaciones DMTF para WS-Management: **www.dmtf.org/standards/wbem/wsman** Las interfaces de servicios web pueden utilizarse aprovechando la infraestructura cliente, como Windows WinRM y Powershell CLI, utilidades de código fuente abierto como WSManCLI y entornos de programación de aplicaciones como Microsoft .NET. Para establecer una conexión de cliente mediante Microsoft WinRM, la versión mínima requerida es 2.0. Para obtener más información, consulte el artículo de Microsoft, <**support.microsoft.com/kb/968929**>.

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

Inicio del CMC mediante otras herramientas de Systems Management

También es posible iniciar el CMC desde Dell Server Administrator o Dell OpenManage IT Assistant.

Para obtener acceso a la interfaz de la CMC mediante Dell Server Administrator, inicie Server Administrator en la estación de administración. En el árbol del sistema del panel izquierdo de la página de inicio de Server Administrator, haga clic en **System (Sistema)** > **Main System Chassis (Chasis principal del sistema)** > **Remote Access Controller (Controladora de acceso remoto)**. Para obtener más información, consulte *Dell Server Administrator User's Guide (Guía del usuario de Server Administrator)*.

Descarga y actualización de firmware del CMC

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

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

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

Establezca el nombre del chasis y su ubicación en un centro de datos para poder identificarlo en la red (el nombre predeterminado es **Dell Rack System**). 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 del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Configuración** > **General**.
   Aparecerá la página **Configuración general del chasis**.
2. Escriba las propiedades de la ubicación y el nombre del chasis. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

   NOTA: El campo Chassis Location (Ubicación del chasis) es opcional. Se recomienda usar los campos **Data Center (Centro de datos)**, **Aisle (Pasillo)**, **Rack (Bastidor)** y **Rack Slot (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, la ubicación y la fecha y hora del chasis mediante la interfaz de línea de comandos, consulte los comandos **setsysinfo** y **setchassisname**. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Establecimiento de la fecha y la hora en el CMC

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

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

Para establecer la fecha y la hora en el CMC mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a Chassis Overview (Descripción general del chasis) y haga clic en **Setup (Configuración)** > **Date/Time (Fecha/Hora)**.
   Aparecerá la página **Fecha/Hora**.
2. Para sincronizar la fecha y la hora con un servidor de protocolo de hora de red (NTP), seleccione **Activar NTP** y especifique hasta tres servidores NTP.
3. Para establecer la fecha y la hora manualmente, desactive **Activar NTP** y edite los campos **Fecha** y **Hora**, seleccione una opción de **Zona horaria** en el menú desplegable y haga clic en **Aplicar**.

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

Para establecer la fecha y la hora con la interfaz de línea de comandos, consulte las secciones sobre el comando config y el grupo de propiedades de base de datos `cfgRemoteHosts` en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command*

Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

Configuración de los LED para identificar componentes en el chasis

Se pueden configurar los LED de todos los componentes o de componentes individuales (el chasis, los servidores y los módulos de E/S) para que parpadeen con el fin de identificar el componente en el chasis.

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

Configuración del parpadeo de LED mediante la interfaz web del CMC

Para activar el parpadeo de uno, varios o todos los LED de los componentes mediante la interfaz web del CMC:

1. Desplácese a cualquiera de las siguientes páginas:
   - **Descripción general del chasis** > **Solución de problemas** > **Identificar**.
   - **Descripción general del chasis** > **Controladora del chasis** > **Solución de problemas** > **Identificar**.
   - **Descripción general del chasis** > **Descripción general del servidor** > **Solución de problemas** > **Identificar**.

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

     Aparecerá la página **Identificar**.
2. Para activar el parpadeo del LED de un componente, seleccione el componente necesario y haga clic en **Parpadear**.
3. Para desactivar el parpadeo del LED de un componente, anule la selección del componente necesario y haga clic en **Dejar de hacer 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 cuyos LED desee configurar. Las opciones de configuración son:

- `server-nx` donde *n* = 1-8 y *x* = a, b, c, o d
- `switch-n` donde *n*=1-6
- `cmc-active`

y *<ledState>* especifica si el LED debe parpadear. Las opciones de configuración son:

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

Configuración de las propiedades del CMC

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

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

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

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

3. Haga clic en **Aplicar**.

   NOTA: Se usará un inicio basado en DNS para cualquier iDRAC particular solo en los siguientes casos:
   - La configuración del chasis es DNS.
   - El CMC ha detectado que el iDRAC específico está configurado con un nombre de DNS.

Configuración del método de inicio de iDRAC con RACADM

Para actualizar el firmware de la CMC mediante RACADM, utilice el subcomando `cfgRacTuneIdracDNSLaunchEnable`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

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

NOTA: Para realizar los siguientes pasos, debe tener privilegios de **Administrador de configuración del chasis**.

Log in Security (Seguridad de inicio de sesión) le permite configurar los atributos de rango de IP para el inicio de sesión en la CMC mediante la interfaz web de la CMC. Para configurar los atributos de rango de IP con la interfaz web del CMC:

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

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

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

- Bloqueo de usuarios
- Bloqueo de direcciones IP
- Cantidad de intentos de inicio de sesión permitidos
- Periodo de tiempo dentro del cual se producirán los conteos de bloqueo por inicio de sesión fallido
- Bloqueo por tiempo de penalidad
- Para activar la función de bloqueo de usuarios, use:

```
racadm config -g cfgRacTuning -o  cfgRacTuneUserBlkEnable <0|1>
```

- Para activar la función de bloqueo de direcciones IP, use:

```
racadm config -g cfgRacTuning -o cfgRacTuneIPBlkEnable <0|1>
```

- Para especificar la cantidad de intentos de inicio de sesión, use:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount
```

- Para especificar el periodo de tiempo dentro del cual deben producirse los conteos de bloqueo por inicio de sesión fallido, use:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow
```

- Para especificar el valor del bloqueo por tiempo de penalidad, use:

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime
```

Para obtener más información acerca de estos objetos, consulte *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Descripción del entorno de CMC redundante

Puede instalar una CMC en espera que tome el control si falla la CMC activa. La CMC redundante puede preinstalarse o se puede instalar posteriormente. Es importante que la red de la CMC esté cableada correctamente para garantizar redundancia total y rendimiento óptimo.

Las protecciones contra fallas pueden ocurrir cuando:

- Ejecute el comando RACADM **cmcchangeover**. Consulte la sección del comando **cmcchangeover** en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.
- Ejecute el comando RACADM racreset en la CMC activa. Consulte la sección del comando **racreset** en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.
- Restablezca la CMC activa desde la interfaz web. Consulte la opción **Reset CMC (Restablecer la CMC)** para **Power Control Operations (Operaciones de control de alimentación)** que se describe en Ejecución de las operaciones de control de alimentación.
- Desconecta el cable de red del CMC activo.
- Desmonta el CMC activo del chasis.
- Inicia una actualización del firmware del CMC en el CMC activo.
- Cuenta con un CMC activo que ya no está en estado funcional.

NOTA: En caso de una protección contra fallas en la CMC, se perderán todas las conexiones de la iDRAC y todas las sesiones de la CMC activa. Los usuarios que hayan perdido su sesión deberán volver a conectarse a la nueva CMC activa.

Conceptos relacionados

Acerca del CMC en espera en la página 36
Modo a prueba de fallos de CMC en la página 36
Proceso de elección del CMC activo en la página 37
Obtención del estado de condición del CMC redundante en la página 37

Acerca del CMC en espera

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

La CMC en espera adopta las mismas propiedades y la misma configuración que la CMC activa. Mantenga la misma versión de firmware en ambas CMC, pero no necesita duplicar la configuración en la CMC en espera.

NOTA: Para obtener información acerca de la instalación de una CMC en espera, consulte *Hardware Owner's Manual (Manual del propietario de hardware)*. Para ver instrucciones para la instalación del firmware de la CMC en su CMC en espera, consulte Actualización del firmware.

Modo a prueba de fallos de CMC

El gabinete M1000e habilita el modo a prueba de fallas para proteger los módulos de E/S y los servidores blade. El modo a prueba de errores se habilita cuando no hay ninguna CMC controlando el chasis. Durante el período de conmutación por error de la CMC o durante la pérdida de administración de una sola CMC:

- No se pueden activar los sistemas blade recién instalados.
- No es posible obtener acceso a los sistemas blade existentes de manera remota.

- Los ventiladores de enfriamiento del chasis funcionan al 100 % para garantizar la protección térmica de los componentes.
- El rendimiento de blade se reduce para limitar el consumo de energía hasta que se restaure la administración del CMC.

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

- Extracción del CMC: la administración del chasis se reanuda después de que se reemplaza el CMC o se ejecuta una protección contra fallas al CMC en espera.
- Extracción del cable de red de la CMC o pérdida de la conexión de red: La administración del chasis se reanuda después de que el chasis cede el control a la CMC en espera después de una falla. La conmutación de red en caso de falla solo se activa en el modo de CMC redundante.
- Restablecimiento del CMC: la administración del chasis se reanuda después de que se reinicia el CMC o el chasis cede el control al CMC en espera después de una falla.
- Emisión del comando de protección contra fallas del CMC: la administración del chasis se reanuda después de que el chasis cede el control al CMC en espera después de una falla.
- Actualización del firmware de la CMC: La administración del chasis se reanuda después de que se reinicia la CMC o el chasis cede el control a la CMC en espera después de una falla. Se recomienda actualizar primero la CMC en espera, de manera que solo haya un suceso de conmutación por falla.
- Detección y corrección de errores del CMC: la administración del chasis se reanuda después de que se reinicia el CMC o el chasis cede el control al CMC en espera después de una falla.

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

Proceso de elección del CMC activo

No hay ninguna diferencia entre las dos ranuras de CMC; es decir, la ranura no indica prioridad. En cambio, la CMC que se instala o se inicia primero asume la función de CMC activa. Si se aplica alimentación de CA con dos CMC instaladas, la instalada en la ranura 1 del chasis de CMC (la de la izquierda) generalmente se convierte en la activa. El CMC activo está indicado con un LED azul.

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

Obtención del estado de condición del CMC redundante

Puede ver la condición de la CMC en espera en la interfaz web. Para obtener más información sobre cómo acceder a la condición de la CMC en la interfaz web, consulte Visualización de información del chasis y supervisión de la condición de los componentes y del chasis.

3

Inicio de sesión en el CMC

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

Tareas relacionadas

Acceso a la interfaz web del CMC en la página 38
Inicio de sesión en CMC como usuario local, usuario de Active Directory o usuario LDAP en la página 39
Inicio de sesión en el CMC mediante una tarjeta inteligente en la página 40
Inicio de sesión en el CMC mediante inicio de sesión único en la página 40
Antes de iniciar sesión en el CMC mediante una consola serie, Telnet o SSH en la página 41
Acceso al CMC mediante RACADM en la página 41
Inicio de sesión en el CMC mediante la autentificación de clave pública en la página 42

Temas:

Acceso a la interfaz web del CMC

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

NOTA: Si usa Microsoft Internet Explorer, con conexión a través de un proxy y recibe el error "The XML page cannot be displayed" (La página XML no se puede mostrar), deberá desactivar el proxy para continuar.

Para acceder a la interfaz web del CMC:

1. Abra una ventana de un explorador web compatible.
   Para obtener la última información sobre los exploradores web compatibles, consulte *Léame* ubicado en **dell.com/support/manuals**.
2. En el campo **Dirección**, escriba la siguiente dirección URL y presione Intro:
   - Para acceder a la CMC mediante una 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 una dirección IPv6: `https://[<CMC IP address>]`

     Si el número de puerto HTTPS predeterminado (puerto 443) se ha cambiado, escriba: `https://[<CMC IP address>]:<port number>`

     NOTA: Cuando utilice IPv6, deberá poner el valor de *<Dirección IP de CMC>* entre corchetes ([ ]).

     donde *<Dirección IP de CMC>* es la dirección IP del CMC y *<Número de puerto>* es el número de puerto HTTPS.

Se visualiza la página de **CMC Login** (Inicio de sesión de la CMC).

Tareas relacionadas

Configuración de un explorador web en la página 26
Inicio de sesión en CMC como usuario local, usuario de Active Directory o usuario LDAP en la página 39
Inicio de sesión en el CMC mediante una tarjeta inteligente en la página 40
Inicio de sesión en el CMC mediante inicio de sesión único en la página 40

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

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

NOTA:

- Para una mayor seguridad, se recomienda encarecidamente cambiar la contraseña predeterminada de la cuenta raíz durante la configuración inicial.
- Cuando se activa la validación de certificados, se debe proporcionar el nombre de dominio completo (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 no se completará.

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

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: Configuración de dominio múltiples para el CMC:

- El esquema se debe extender en todos los dominios secundarios del bosque.
- Se debe agregar el usuario a cada dominio y se debe crear el dispositivo del CMC en cada dominio.
- Al configurar el esquema extendido de la CMC, se debe mencionar el dominio que se está configurando. Por ejemplo, si el dominio raíz es **fwad2.lab** y el usuario es **cmcuser5@NodeA.GrandChildA.SubChildA.ChildA.fwad2.lab**, el dominio donde está configurado el usuario es **NodeA.GrandChildA.SubChildA.ChildA.fwad2.lab**. El usuario **cmcuser5@NodeA.GrandChildA.SubChildA.ChildA.fwad2.lab** se puede validar desde la CMC.

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

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

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

   NOTA: Este campo distingue entre mayúsculas y minúsculas.
3. En el campo **Dominio**, en el menú desplegable, seleccione el dominio requerido.
4. También tiene la opción de seleccionar un límite de tiempo de espera para la sesión. Se trata del período durante el cual puede permanecer conectado sin actividad antes de que se cierre la sesión automáticamente. El valor predeterminado es el tiempo de espera en inactividad de los servicios web.
5. Haga clic en **OK** (Aceptar).

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

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.

NOTA: Para la autentificación LDAP por OPEN-DS, la clave DH debe ser mayor que 768 bits.

Conceptos relacionados

Configuración de cuentas de usuario y privilegios en la página 131

Tareas relacionadas

Acceso a la interfaz web del CMC en la página 38

Inicio de sesión en el CMC mediante una tarjeta inteligente

Puede iniciar sesión en la CMC mediante una tarjeta inteligente. Las tarjetas inteligentes proporcionan autenticación de dos factores (TFA) para tener 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 puede utilizar la dirección IP para iniciar sesión en la CMC con el inicio de sesión de tarjeta inteligente. Kerberos valida las credenciales en función del nombre de dominio completo (FQDN).

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

- Cargar un certificado de una autoridad de certificados (CA) de confianza (certificado de Active Directory firmado por una autoridad de certificados) en el 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 el CMC como usuario de Active Directory mediante una tarjeta inteligente:

1. Inicie sesión en la CMC mediante el vínculo `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), ingrese 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**.
   Aparece la página 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.

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

Tareas relacionadas

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory en la página 158

Inicio de sesión en el CMC mediante inicio de sesión único

Cuando se activa el inicio de sesión único (SSO), es posible iniciar sesión en el CMC sin introducir las credenciales de autentificación de usuario del dominio, como el nombre de usuario y la contraseña.

NOTA: No puede emplear la dirección IP para utilizar el inicio de sesión único. Kerberos valida sus credenciales en función del FQDN.

Antes de iniciar sesión en el CMC mediante el inicio de sesión único, asegúrese de lo siguiente:

- 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 el CMC mediante el 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 mediante: `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), acceda a la interfaz web de la CMC mediante `<cmcname.domain-name>:<port number>`, donde **cmcname** es el nombre de host de la CMC, **domain-name** es el nombre del dominio y **port number** es el número del puerto HTTPS.

   La CMC lo conectará utilizando las credenciales Kerberos que el navegador almacenó en caché cuando inició sesión utilizando su cuenta válida de Active Directory. Si la conexión falla, el navegador va a la página de inicio de sesión normal de la CMC.

   NOTA: Si no inició sesión en el dominio de Active Directory y está utilizando un explorador que no es Internet Explorer, la conexión fallará y el explorador mostrará solamente una página en blanco.

Tareas relacionadas

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory en la página 158

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

Es posible iniciar sesión en el CMC mediante una conexión serie, Telnet o SSH, o por medio de Dell CMC Console en el iKVM.

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

1. Inicie sesión en el CMC con el software de emulación de terminal de la estación de administración.
2. Escriba su nombre de usuario y contraseña para el CMC y presione <Intro>.
   Ahora está conectado al CMC.

   Además, consulte los siguientes temas:
   - Uso de una consola Telnet con el CMC
   - Uso de SSH con el CMC
   - Configuración requerida de Minicom

Tareas relacionadas

Configuración del CMC para el uso de consolas de línea de comandos en la página 160
Activación del acceso al iKVM desde Dell CMC Console en la página 209

Acceso al CMC mediante RACADM

RACADM proporciona un conjunto de comandos que permiten configurar y administrar la CMC mediante una interfaz de texto. Se puede acceder a RACADM por medio de una conexión Telnet/SSH o serie, a través de Dell CMC Console en el iKVM, o de manera remota mediante la interfaz de línea de comandos RACADM instalada en una estación de administración.

La interfaz RACADM se clasifica de la siguiente manera:

- RACADM remoto: permite ejecutar comandos RACADM en una estación de administración con la opción -r y el nombre DNS o la dirección IP del CMC.
- RACADM de firmware: Permite iniciar sesión en la CMC por medio de una conexión serie, Telnet o SSH, o el iKVM. Con RACADM de firmware, se puede ejecutar la implementación de RACADM que forma parte del firmware de la CMC.

NOTA: RACADM remoto se incluye en el DVD Dell Systems Management Tools and Documentation y se instala en una estación de administración.

Puede utilizar comandos de RACADM remoto en secuencias de comandos para configurar varias CMC. La CMC no admite secuencias de comandos. Por ende, no se puede ejecutar las secuencias de comandos directamente en la CMC.

Para obtener más información acerca de RACADM, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

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

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

Puede 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.

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 se utiliza una frase de contraseña con las claves, los clientes tanto Windows como Linux ofrecen métodos para automatizar eso también. Para los clientes Windows, se puede usar la aplicación Pageant. Esta aplicación se ejecuta en segundo plano y hace que la introducción de la frase de contraseña sea transparente. Para los clientes Linux, se puede utilizar sshagent. Para configurar y utilizar cualquiera de estas aplicaciones, consulte la documentación que las acompaña.

Conceptos relacionados

Configuración de la autentificación de clave pública en SSH en la página 162

Varias sesiones en el CMC

En la tabla siguiente se proporciona una lista de varias sesiones posibles en el CMC mediante las distintas interfaces.

Tabla 9. Varias sesiones en el CMC

Interfaz	Máximo de sesiones por interfaz
Interfaz web del CMC	4
RACADM	4
Telnet	4
SSH	4
WS-MAN	4
iKVM	1
Serie	1

Cambio de la contraseña de inicio de sesión predeterminada

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

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

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

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

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

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

Cuando inicia sesión en la interfaz web de la CMC, si aparece la página **Default Password Warning (Advertencia de contraseña predeterminada)**, puede cambiar la contraseña. Para hacerlo:

1. Seleccione la opción **Cambiar contraseña predeterminada**.
2. En el campo **Contraseña nueva**, escriba la contraseña nueva.

   La cantidad máxima de caracteres para la contraseña es 20. Los caracteres están enmascarados. Se admiten los siguientes caracteres:
   - 0-9
   - A-Z
   - a-z
   - Caracteres especiales: +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, l, \
3. En el campo **Confirmar contraseña**, escriba nuevamente la contraseña.
4. Haga clic en **Continue (Continuar)**. Se configurará la contraseña nueva e iniciará sesión en la CMC.

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

   Para obtener información acerca del resto de los campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM

Para cambiar la contraseña, ejecute el siguiente comando RACADM:

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

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

Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

Activación o desactivación del mensaje de advertencia de contraseña predeterminada

Puede activar o desactivar la presentación del mensaje de advertencia de contraseña predeterminada. Para cambiar esto, debe contar con el privilegio de configuración de usuarios.

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

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

1. Diríjase a **Controladora del chasis** > **Autentificación de usuarios** > **Usuarios locales**.
   Se muestra la página **Users (Usuarios)**.
2. En la sección **Default Password Warning (Advertencia de contraseña predeterminada)**, seleccione **Enable (Activar)**, y luego haga clic en **Apply (Aplicar)** para activar la visualización de la página **Default Password Warning (Advertencia de contraseña predeterminada)** al iniciar sesión en la CMC. De lo contrario, seleccione **Disable (Desactivar)**.

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

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

Para activar la visualización del mensaje de advertencia para cambiar la contraseña de inicio de sesión predeterminada mediante RACADM, utilice el objeto `racadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> or <1>`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

4

Actualización de firmware

Es posible actualizar el firmware para los siguientes elementos:

- CMC: activo y en espera
- iKVM
- Módulos de E/S

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

- IDRAC: Las iDRAC anteriores a iDRAC6 se deben actualizar mediante la interfaz de recuperación. El firmware de iDRAC6 también se puede actualizar con la interfaz de recuperación, pero es obsoleto para iDRAC6 y las versiones futuras.
- BIOS
- Unified Server Configurator
- Diagnósticos de 32 bits
- Driver Pack del SO
- Controladoras de interfaz de red
- Controladoras RAID

Conceptos relacionados

Descarga de firmware del CMC en la página 45
Visualización de versiones de firmware actualmente instaladas en la página 46
Actualización de firmware del CMC en la página 47
Actualización de firmware del iKVM en la página 48
Actualización de firmware de los componentes del servidor en la página 51
Recuperación de firmware del iDRAC mediante el CMC en la página 66
Actualización de firmware de los dispositivos de infraestructura de módulo de E/S en la página 49

Temas:

Descarga de firmware del CMC

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

En el paquete de firmware del CMC, se incluyen los siguientes componentes de software:

- Datos y código de firmware compilado de la CMC
- Interfaz web, JPEG y otros archivos de datos de la interfaz de usuario
- Archivos de configuración predeterminados

Como alternativa, utilice Dell Repository Manager (DRM) para buscar las actualizaciones de firmware disponibles más recientes. Dell Repository Manager (DRM) garantiza que los sistemas Dell estén actualizados con la última versión del BIOS, los controladores, el firmware y el software. Puede buscar las actualizaciones disponibles más recientes para las plataformas admitidas en el sitio de asistencia

(**support.dell.com**), por marca y modelo, o por etiqueta de servicio. Puede descargar las actualizaciones o crear un repositorio a partir de los resultados de la búsqueda. Para obtener más información sobre el uso de DRM para buscar las actualizaciones de firmware más recientes, consulte Using Dell Repository Manager to Search for the Latest Updates on the Dell Support Site (Uso de Dell Repository Manager para buscar las actualizaciones más recientes en el sitio de asistencia de Dell) en Dell Tech Center. Para obtener información sobre cómo guardar el archivo de inventario que DRM utiliza como entrada para crear los repositorios, consulte Cómo guardar el informe de inventario del chasis mediante la interfaz web de la CMC. Se recomienda actualizar el firmware del chasis M1000e en el siguiente orden:

- El firmware de los componentes de blade
- Firmware de la CMC

Para obtener más información sobre la secuencia de actualización para el chasis M1000e, consulte *CMC Firmware 5.0 Release Notes* (Notas de la versión del firmware del CMC 5.0) en el sitio de asistencia.

Imagen de firmware del CMC firmado

Para la CMC de M1000e 5.0 y versiones posteriores, el firmware 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 verificación de la firma se puede llevar a cabo en las versiones de firmware 3.1 y posteriores. Para regresar el firmware a las versiones de la CMC de M1000e anteriores a la 3.1, primero actualice el firmware con la versión 3.1 o una posterior, pero anterior a 5.0. Después de esta actualización, se puede regresar a firmware anterior de la CMC de M1000e de versiones no firmadas. Las CMC 5.0 y posteriores llevan la firma como parte de la imagen, y también tienen los archivos de firma de las versiones 3.10, 3.20, 3.21, 4.0, 4.10, 4.11, 4.30, 4.31, 4.45 y 4.5 únicamente. Por lo tanto, la actualización del firmware de la CMC solo se admite para dichas versiones. Con cualquier otra versión, primeramente realice la actualización a cualquiera de estas versiones y luego realice la actualización a la versión requerida.

Visualización de versiones de firmware actualmente instaladas

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

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

En la interfaz web del CMC, desplácese 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** > **Actualizar**
- **Chassis Overview (Descripción general del chasis)** > **I/O Module Overview (Descripción general del módulo de E/S)** > **Update (Actualizar)**
- **Descripción general del chasis** > **iKVM** > **Actualizar**

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 el CMC detecta que un iDRAC contiene firmware dañado, el iDRAC de la generación anterior también aparece en la página Actualización del firmware.

Visualización de versiones de firmware actualmente instaladas mediante RACADM

Para ver las versiones de firmware instaladas actualmente mediante RACADM, utilice el subcomando **getkvminfo**. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

Actualización de firmware del CMC

Puede actualizar el firmware de la CMC mediante la interfaz web o RACADM. De forma predeterminada, la actualización de firmware conserva la configuración actual de la CMC. Durante el proceso de actualización, puede restablecer la configuración predeterminada de fábrica de la CMC.

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

Si se utiliza una sesión de interfaz de usuario web para actualizar el firmware de los componentes del sistema, se debe establecer un valor suficientemente elevado de tiempo de espera en inactividad, para acomodarse a lo que demora la transferencia de los archivos. En algunos casos, es posible que el tiempo de transferencia de archivos de firmware sea de hasta 30 minutos. Para configurar el 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 al 100%.

Si hay CMC redundantes instaladas en el chasis, se recomienda actualizar las dos CMC con la misma versión de firmware, al mismo tiempo y en una misma operación. Si las CMC tienen versiones diferentes de firmware y se produce una protección contra fallas, se pueden generar resultados inesperados.

NOTA: La actualización o reversión del firmware de las CMC solo se ofrece para las versiones de firmware 3.10, 3,20, 3.21, 4.0, 4.10, 4.11, 4,30, 4,31, 4.45, 4.5, 5.0 y posteriores. Con cualquier otra versión, primeramente realice la actualización a cualquiera de estas versiones y luego realice la actualización a la versión requerida.

Una vez que se ha cargado el firmware correctamente, la CMC activa se restablece y temporalmente deja de estar disponible. Si existe una CMC en espera, las CMC intercambian roles. La CMC en espera se convierte en la activa. Si se aplica una actualización solo a la CMC activa, después del restablecimiento, la CMC activa no ejecutará la imagen actualizada, ya que solo la CMC en espera posee dicha imagen. En general, se recomienda enfáticamente tener versiones de firmware idénticas en las CMC activa y en espera.

Cuando se haya actualizado la CMC en espera, intercambie los roles de las CMC para que la recién actualizada se convierta en la activa y la de la versión de firmware más antigua quede en espera. Consulte la sección del comando `cmcchangeover` en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)* para obtener información sobre el intercambio de roles. Esto le permitirá verificar que la actualización se haya realizado correctamente y que el nuevo firmware funcione bien, antes de actualizar el firmware de la segunda CMC. Cuando ambas CMC se hayan actualizado, puede usar el comando `cmcchangeover` para restaurar los roles anteriores de las CMC. La revisión del firmware de CMC 2.x actualiza la CMC principal y la redundante sin usar el comando. `cmcchangeover`.

Para evitar la desconexión de otros usuarios durante el restablecimiento, notifique a los usuarios autorizados que puedan conectarse a las CMC y busque sesiones activas en la página Sessions (Sesiones). Para abrir la página **Sessions (Sesiones)**, seleccione **Chassis (Chasis)** en el árbol, haga clic en la ficha **Network (Red)** y luego haga clic en la subficha **Sessions (Sesiones)**.

Durante las etapas finales del proceso de actualización del firmware de CMC, la sesión del navegador y la conexión con la CMC se pierden temporalmente debido a que la CMC no está conectada a la red. La CMC deja en estado crítico la condición general del chasis debido a la pérdida temporal de la red. Cuando se reinicie la CMC después de unos minutos, inicie sesión. La CMC informará el buen estado de la condición general del chasis y el enlace de red de la CMC estará activo. Una vez se haya restablecido, aparecerá la nueva versión del firmware en la página **Actualización del firmware**.

Al transferir archivos hacia y desde las CMC, se ve girar el icono de transferencia de archivos. Si el icono es animado, asegúrese de que su navegador esté configurado para permitir animaciones. Para ver instrucciones, consulte Cómo permitir animaciones en Internet Explorer.

Si experimenta problemas al descargar archivos desde la CMC mediante Internet Explorer, active la opción No guardar las páginas cifradas en el disco. Para ver instrucciones, consulte Descarga de archivos desde la CMC con Internet Explorer.

Conceptos relacionados

Descarga de firmware del CMC en la página 45
Visualización de versiones de firmware actualmente instaladas en la página 46

Actualización de firmware del CMC mediante la interfaz web

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

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

- **Chassis Overview (Descripción general del chasis)** > **I/O Module Overview (Descripción general del módulo de E/S)** > **Update (Actualizar)**
- **Chassis Overview (Descripción general del chasis)** > **iKVM** > **Update (Actualizar)**

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

2. En la sección **Firmware del CMC**, active las casillas de la columna **Actualizar destinos** para el o los CMC (si existe un CMC en espera presente) cuyo firmware desea actualizar y haga clic en **Aplicar actualización de CMC**.
3. En el campo **Firmware Image (Imagen del firmware)**, escriba la ruta de acceso del archivo de la imagen del firmware en la estación de administración o la red compartida, o bien, haga clic en **Browse (Examinar)** para buscar la ubicación del archivo. El nombre predeterminado de la imagen del firmware de la CMC es `firmimg.cmc`.
4. Haga clic en **Iniciar actualización del firmware** y, a continuación, en **Sí** para continuar. 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.

   NOTA: Si el chasis admite unidades de suministro de energía de CC, aparece un mensaje de error si intenta actualizar el firmware a una versión no compatible con una unidad de suministro de energía de CC.

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

   NOTA: Es posible que la actualización del CMC tarde varios minutos.

6. En una CMC en espera, cuando se completa la actualización, en el campo **Update State (Estado de la actualización)** se indica **Done (Finalizada)**. En una CMC activa, durante las etapas finales del proceso de actualización del firmware, la sesión del navegador y la conexión con la CMC se perderán temporalmente debido a que la CMC queda fuera de línea. Debe iniciar sesión nuevamente pasados unos minutos, cuando la CMC activa se haya reiniciado. Una vez restablecida la CMC, aparecerá la nueva versión del firmware en la página **Firmware Update (Actualización del firmware)**.

   NOTA: Después de actualizar el firmware, borre la memoria caché del navegador web. Para obtener instrucciones para borrar la memoria caché del navegador, consulte la ayuda en línea de su navegador.

Actualización de firmware de la CMC mediante RACADM

Para actualizar el firmware de la CMC mediante RACADM, utilice el subcomando `fwupdate`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

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

Actualización de firmware del iKVM

Una vez que se haya cargado correctamente el firmware, el iKVM se restablecerá y dejará de estar disponible temporalmente.

Conceptos relacionados

Descarga de firmware del CMC en la página 45
Visualización de versiones de firmware actualmente instaladas en la página 46

Actualización de firmware del iKVM mediante la interfaz web del CMC

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

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

- **Descripción general del chasis** > **iKVM** > **Actualizar**

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

2. En la sección **Firmware de iKVM**, seleccione la casilla de verificación de la columna **Actualizar destinos** para el **iKVM** cuyo firmware desea actualizar y haga clic en **Aplicar actualización de iKVM**.
3. En el campo **Firmware Image (Imagen del firmware)**, escriba la ruta de acceso del archivo de la imagen del firmware en la estación de administración o la red compartida, o bien, haga clic en **Browse (Examinar)** para buscar la ubicación del archivo. El nombre predeterminado de la imagen del firmware de iKVM es `iKVM.bin`.
4. Haga clic en **Iniciar actualización del firmware** y, a continuación, en **Sí** para continuar.

   La sección **Progreso de actualización del firmware** proporciona información sobre el estado de la actualización de firmware. Aparecerá un indicador de estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización de firmware.
5. Instrucciones adicionales que hay que seguir:
   - No haga clic en el icono **Actualizar** ni visite otra página durante la transferencia de archivos.
   - Para cancelar el proceso, haga clic en **Cancelar transferencia y actualización de archivos**. Esta opción solo está disponible durante la transferencia de archivos.
   - El campo **Estado de la actualización** muestra el estado de la actualización de firmware.

   NOTA: La actualización del iKVM puede demorar hasta dos minutos.

   Cuando se completa la actualización, el iKVM se reinicia y el nuevo firmware aparece en la página **Actualización del firmware**.

Actualización de firmware del iKVM mediante RADCAM

Para actualizar el firmware del iKVM mediante RACADM, utilice el subcomando `fwupdate`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

Actualización de firmware de los dispositivos de infraestructura de módulo de E/S

Al realizar esta actualización, se actualiza el firmware de un componente del dispositivo módulo de E/S, pero no el firmware del dispositivo en sí; el componente es el circuito de interfaz entre el dispositivo módulo de E/S y la CMC. La imagen de actualización del componente reside en el sistema de archivos de la CMC, y el componente se visualiza como un dispositivo actualizable en la interfaz web de la CMC solamente si la revisión actual del componente y la imagen del componente en la CMC no coinciden.

Antes de actualizar el firmware de un dispositivo de infraestructura de módulo de E/S, asegúrese de que se haya actualizado el firmware del CMC.

NOTA:

La CMC permite las actualizaciones del firmware de dispositivos de infraestructura de módulo de E/S (IOMINF) solamente si detecta que el firmware IOMINF está desactualizado con respecto a la imagen almacenada en el sistema de archivos de la CMC. Si el firmware IOMINF está actualizado, la CMC impide las actualizaciones de IOMINF. Los dispositivos de IOMINF actualizado no figuran como dispositivos actualizables.

Conceptos relacionados

Descarga de firmware del CMC en la página 45
Visualización de versiones de firmware actualmente instaladas en la página 46
Actualización de software de módulo de E/S mediante la interfaz web del CMC en la página 189

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

Para actualizar el firmware de los dispositivos de infraestructura de módulo de E/S, en la interfaz web del 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 lo contrario, desplácese a cualquiera de las siguientes páginas:

   - **Descripción general del chasis** > **Actualizar** > **Coprocesador del módulo de E/S**
   - **Descripción general del chasis** > **Firmware del CMC** > **Aplicar actualización del CMC** > **Coprocesador del módulo de E/S**
   - **Descripción general del chasis** > **Firmware del iKVM** > **Aplicar actualización del iKVM** > **Coprocesador del módulo de E/S**

   Aparece la página **Actualización de firmware**, que proporciona un vínculo para acceder a la página **Actualización del firmware del módulo de E/S**.

2. En la página **Actualización del firmware del módulo de E/S**, en la sección **Firmware del módulo de E/S**, seleccione la casilla de verificación de la columna **Actualizar** para el módulo de E/S cuyo firmware desea actualizar y haga clic en **Aplicar actualización de firmware**.
   En la sección **Update Status (Estado de actualización)** se brinda información sobre el estado de la actualización del firmware. Aparecerá un indicador de estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar 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.
   - El cronómetro de transferencia de archivos no se muestra cuando se actualiza el firmware de un dispositivo de infraestructura de módulo de E/S.
   - Si el coprocesador del módulo de E/S tiene la versión de firmware más reciente, la casilla de verificación no se muestra en la columna **Actualizar** .

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

Actualización de firmware de módulo de E/S mediante RACADM

Para actualizar el firmware de dispositivos de infraestructura de módulos de E/S mediante RACADM, utilice el subcomando fwupdate. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Actualización de firmware del iDRAC del servidor mediante la interfaz web

Para actualizar el firmware del iDRAC en el servidor mediante la interfaz web del CMC:

1. Desplácese a cualquiera de las siguientes páginas:
   - **Descripción general del chasis** > **Actualizar**
   - **Descripción general del chasis** > **Controladora del chasis** > **Actualizar**
   - **Descripción general del chasis** > **Descripción general del módulo de E/S** > **Actualizar**
   - **Descripción general del chasis** > **iKVM** > **Actualizar**

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

   También es posible actualizar el firmware de la iDRAC del servidor desde **Chassis Overview (Descripción general del chasis)** > **Server Overview (Descripción general del servidor)** > **Update (Actualizar)**. Para obtener más información, consulte Actualización del firmware de los componentes de servidores.
2. Para actualizar el firmware del iDRAC, en la sección **Firmware de iDRAC Enterprise**, seleccione la casilla de verificación de la columna **Actualizar destinos** para el iKVM cuyo firmware desea actualizar, haga clic en **Aplicar actualización de iDRAC Enterprise** y desplácese al paso 4.
3. Para actualizar el firmware del iDRAC, en la sección **Firmware de iDRAC Enterprise**, haga clic en el vínculo **Actualizar** para el servidor cuyo firmware desea actualizar.
   Aparecerá la página **Actualización de los componentes del servidor**. Para continuar, consulte la sección Actualización del firmware de los componentes de servidores.

4. En el campo **Firmware Image (Imagen del firmware)**, escriba la ruta de acceso del archivo de la imagen del firmware en la estación de administración o la red compartida, o bien, haga clic en **Browse (Examinar)** para buscar la ubicación del archivo. El nombre predeterminado de la imagen del firmware de la iDRAC es `firming.imc`.
5. Haga clic en **Iniciar actualización del firmware** y, a continuación, en **Sí** para continuar.

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

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

   Cuando se completa la actualización, el iKVM se reinicia y el nuevo firmware aparece en la página **Actualización del firmware**.

Actualización de firmware del iDRAC del servidor mediante RACADM

Para actualizar el firmware de la iDRAC mediante RACADM, utilice el subcomando fwupdate. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide for iDRAC and CMC (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e para iDRAC y CMC)*.

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.

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

- Servidores de 11.ª generación: después de reiniciar el servidor, en los valores de Ctrl-E, seleccione **Servicios del sistema**, active **CSIOR** y guarde los cambios.
- Servidores de 12ª generación y posteriores: después de reiniciar el servidor, en los valores de F2, seleccione **Configuración del iDRAC** > **Lifecycle Controller**, active **CSIOR** y guarde los cambios.

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:

- Al seleccionar componentes individuales en el servidor para la actualización, asegúrese de que no existan dependencias entre los componentes seleccionados. La selección de algunos componentes con dependencias en otros componentes para la actualización puede detener de forma abrupta el funcionamiento del servidor.
- Asegúrese de actualizar los componentes del servidor en el orden que se recomienda. De lo contrario, es posible que el proceso de actualización de firmware de los componentes no se complete correctamente. Para obtener más información sobre cómo actualizar el firmware de componentes del servidor, consulte Flujo de trabajo recomendado para realizar actualizaciones en los servidores PowerEdge.

El método de actualización de todo el servidor blade con un solo clic o el método **Update from Network Share (Actualizar desde recurso compartido de red)** le permite actualizar el firmware de los componentes del servidor mediante archivos DUP almacenados en un recurso compartido de red. Puede usar la función de actualización basada en Dell Repository Manager (DRM) para acceder a los

archivos DUP almacenados en un recurso compartido de red y actualizar los componentes del servidor en una sola operación. Puede configurar un repositorio remoto personalizado de imágenes binarias y DUP de firmware, a través de Dell Repository Manager, para compartirlo en el recurso compartido de red.

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

- Permite actualizar todos los componentes de todos los servidores blade con una cantidad mínima de clics.
- Todas las actualizaciones se encuentran en paquetes en el directorio. De esta manera, no es necesario cargar de forma individual el firmware de cada uno de los componentes.
- Método más rápido y consistente para actualizar los componentes del servidor
- Permite mantener una imagen estándar con las versiones de actualización necesarias para los componentes del servidor que se pueden usar para actualizar varios servidores en una única operación.
- Es posible copiar los directorios de las actualizaciones con la herramienta Dell Server Update Utility (SUU), descargar DVD o crear y personalizar las versiones de actualización necesarias en Dell Repository Manager (DRM). No se necesita la versión más reciente de Dell Repository Manager para crear este directorio. Sin embargo, DRM versión 1.8 ofrece una opción para crear un repositorio (directorio de actualizaciones) basado en el inventario de M1000e que se ha exportado. Para obtener más información sobre cómo guardar el informe de inventario del chasis, consulte Cómo guardar el informe de inventario del chasis mediante la interfaz web de la CMC. Para obtener información sobre la creación de un repositorio mediante DRM, consulte *Dell Repository Manager Data Center Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Data Center versión 1.8)* y *Dell Repository Manager Business Client Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Business Client versión 1.8),* disponibles en **dell.com/support/manuals**.

Lifecycle Controller admite la actualización de módulos a través de iDRAC. 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 **Chassis Overview (Descripción general del chasis)** > **Server Overview (Descripción general del servidor)** > **Update (Actualizar)** > **Server Component Update (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.

NOTA: La versión del firmware del iDRAC debe ser 3.2 o posterior para admitir esta función.

Si el servicio Lifecycle Controller está desactivado en el servidor, la sección **Inventario de firmware de componentes y dispositivos** muestra *Lifecycle Controller puede no estar activado*.

Conceptos relacionados

Habilitación de Lifecycle Controller en la página 57
Filtrado de componentes para actualizaciones de firmware en la página 60
Visualización del inventario de firmware en la página 62
Operaciones de Lifecycle Controller en la página 64
Actualización de firmware de los dispositivos de infraestructura de módulo de E/S en la página 49

Secuencia de actualización de componentes del servidor

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

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

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

Versiones de firmware admitidas para la actualización de componentes del servidor

En la sección a continuación se detallan las versiones de los componentes admitidas para la actualización de firmware del CMC y la actualización de componentes del servidor.

En la siguiente tabla se indican las versiones de firmware admitidas para los componentes del servidor cuando el firmware de la CMC se actualiza de la versión 5.2 a la 6.0 pero los componentes del servidor no se actualizan a la siguiente versión.

NOTA: La actualización del firmware de la CMC de la versión 5.2 a la 6.0 se realiza correctamente con las versiones N-1 de iDRAC, BIOS y Lifecycle Controller en todos los servidores que se mencionan en la siguiente tabla.

Tabla 10. Versiones de firmware admitidas para los componentes del servidor en una actualización de firmware de la CMC (versión 5.2 a 6.0)

Plataforma	Componente del servidor	Versión actual de cada componente (versión N-1)
M610	iDRAC	3.80 A00
	Lifecycle Controller	1.6.5.12.A00
	Diagnóstico	5158A3
	BIOS	6.3.0
	NIC	7.8.15
M610x	iDRAC	3.80 A00
	Lifecycle Controller	1.6.5.12 A00
	Diagnóstico	5158A3
	BIOS	6.3.0
	NIC	7.8.15
M710	iDRAC	3.80 A00
	Lifecycle Controller	1.6.5.12 A00
	Diagnóstico	5158A3
	BIOS	6.3.0
M910	iDRAC	3.80 A00
	Lifecycle Controller	1.6.5.12 A00
	Diagnóstico	5158A3
	BIOS	2.9.0
M710HD	iDRAC	3.80 A00
	Lifecycle Controller	1.6.5.12 A00
	Diagnóstico	5158A3
	BIOS	7.0.0
	NIC	7.8.15

Tabla 10. Versiones de firmware admitidas para los componentes del servidor en una actualización de firmware de la CMC (versión 5.2 a 6.0) (continuación)

Plataforma	Componente del servidor	Versión actual de cada componente (versión N-1)
M420	iDRAC	2.41.40.40
	Lifecycle Controller	2.41.40.40
	Diagnóstico	4231A0
	BIOS	2.3.3
	NIC	7.8.15
M520	iDRAC	2.41.40.40
	Lifecycle Controller	2.41.40.40
	Diagnóstico	4225A2
	BIOS	2.32
M620	iDRAC	2.41.40.40
	Lifecycle Controller	2.41.40.40
	Diagnóstico	4231A0
	BIOS	2.5.2
	NIC	7.8.15
M820	iDRAC	2.41.40.40
	Lifecycle Controller	2.41.40.40
	Diagnóstico	4231A0
	BIOS	2.3.2
M630	iDRAC	2.41.40.40
	Lifecycle Controller	2.41.40.40
	Diagnóstico	4239.44
	BIOS	2.4.2
M830	iDRAC	2.41.40.40
	Lifecycle Controller	2.41.40.40
	Diagnóstico	4239A16_4239.24
	BIOS	2.4.2

En la siguiente tabla se indican las versiones de firmware admitidas para los componentes del servidor en una situación en la que la versión de firmware de la CMC existente es 6.0 y los componentes del servidor se actualizan de la versión N-1 a la versión N.

NOTA: La actualización de firmware de los componentes del servidor de la versión N-1 a la versión N se realiza correctamente cuando el firmware de la CMC es 5.0 o posterior en todos los servidores de las generaciones 11, 12, 13 y 14 que se mencionan en la siguiente tabla.

Tabla 11. 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)
M610	iDRAC	3.80 A00	3.85 A00
	Lifecycle Controller	1.6.5.12 A00	1.7.5.4
	Diagnóstico	5158A3	5162A0
	BIOS	6.3.0	6.4.0
	NIC	7.8.15	20.6.18
M610x	iDRAC	3.80 A00	3.85 A00
	Lifecycle Controller	1.6.5.12 A00	1.7.5.4
	Diagnóstico	5158A3	5162A0
	BIOS	6.3.0	6.4.0
	NIC	7.8.15	20.6.18
M710	iDRAC	3.80 A00	3.85 A00
	Lifecycle Controller	1.6.5.12 A00	1.7.5.4
	Diagnóstico	5158A3	5162A0
	BIOS	6.3.0	6.4.0
M910	iDRAC	3.80 A00	3.85 A00
	Lifecycle Controller	1.6.5.12 A00	1.7.5.4
	Diagnóstico	5158A3	5162A0
	BIOS	2.9.0	2.10.0
M710HD	iDRAC	3.80 A00	3.85 A00
	Lifecycle Controller	1.6.5.12 A00	1.7.5.4
	Diagnóstico	5158A3	5162A0
	BIOS	7.0.0	8.0.0
	NIC	7.8.15	20.6.18
M420	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnóstico	4231A0	4247A1

Tabla 11. 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	2.3.3	2.4.2
	NIC	7.8.15	20.6.18
M520	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnóstico	4231A0	4247A1
	BIOS	2.3.2	2.4.2
	NIC	7.8.15	20.6.18
M620	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnóstico	4231A0	4247A1
	BIOS	2.5.2	2.5.4
	NIC	7.8.15	20.6.18
M820	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnóstico	4231A0	4742A1
	BIOS	2.3.2	2.3.3
M630	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnóstico	4239.44	4239A36
	BIOS	2.4.2	2.5.4
M830	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnóstico	4239,32	4239A36
	BIOS	2.4.2	2.5.4
M640	iDRAC	No aplicable	3.10.10.10
	Lifecycle Controller	No aplicable	3.10.10.10
	Diagnóstico	No aplicable	4301.13 (YFXV5)
	BIOS	No aplicable	1.0.0

Habilitación de Lifecycle Controller

Es posible activar el servicio Lifecycle Controller durante el proceso de inicio del servidor:

- En la consola de inicio de los servidores iDRAC, cuando aparezca el mensaje `Press <CTRL-E> for Remote Access Setup within 5 sec.`, pulse <CTRL-E>. A continuación, en la pantalla de configuración, active **System Services (Servicios del sistema)**.
- En la consola de inicio de los servidores iDRAC, seleccione F2 para acceder a la configuración del sistema. En la pantalla de configuración, seleccione i**DRAC Settings (Configuración de iDRAC)** y, a continuación, seleccione **System Services (Servicios del sistema)**.

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

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

- *Lifecycle Controller Remote Services User's Guide (Guía del usuario de servicios remotos de Lifecycle Controller)*.
- **delltechcenter.com/page/Lifecycle+Controller**.

La página **Server Component Update (Actualización de componentes del servidor)** le permite actualizar diferentes componentes del firmware en el sistema. Para utilizar las funciones y los recursos de esta página, es necesario tener:

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

Si los privilegios no son suficientes, puede ver el inventario de firmware de los componentes y los dispositivos en el servidor. No puede seleccionar ningún componente o dispositivo 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 del CMC

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

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.
   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione el tipo de método de actualización necesario:
   - **Actualizar desde archivo**
   - **Actualizar desde recurso compartido de red**

Actualización de firmware de los componentes del servidor

El firmware de los componentes de un servidor se puede actualizar mediante el método de archivo o el método de recurso compartido de red.

Puede instalar la versión siguiente de la imagen de firmware para los componentes o los dispositivos seleccionados de uno o varios servidores. La imagen de firmware está disponible dentro de Lifecycle Controller para una operación de reversión.

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.

Vacíe la cola de trabajos antes de inicializar la actualización del firmware de los componentes de un servidor. En la página Lifecycle Controller Jobs (Trabajos de Lifecycle Controller), hay disponible una lista de todos los trabajos de los servidores. Esta página permite borrar uno o varios trabajos, o eliminar todos los trabajos del servidor. Consulte en la sección de resolución de problemas "Administración de trabajos de Lifecycle Controller en un sistema remoto".

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

Si el tamaño de la imagen en el archivo de actualización es mayor, el estado del trabajo indica que se ha producido una falla en la descarga. Si se intentan varias actualizaciones de componentes en un servidor, el tamaño combinado de todos los archivos de actualización de firmware puede superar también los 48 MB. En esos casos, una de las actualizaciones de componentes fracasa al truncarse el archivo de actualización.

Para actualizar varios componentes de un servidor, se recomienda actualizar primero juntos los componentes de Lifecycle Controller y de Diagnósticos de 32 bits. Los demás componentes pueden actualizarse juntos después.

La siguiente tabla enumera los componentes que son compatibles con la función **Actualización del firmware**.

NOTA: Cuando se aplican varias actualizaciones de firmware a través de los métodos fuera de banda o mediante la interfaz web de Lifecycle Controller, las actualizaciones se ordenan de la manera más eficiente posible para reducir el reinicio innecesario de un sistema.

Tabla 12. Actualización del firmware: componentes admitidos

	Nombre del componente	¿Reversión del firmware admitida? (Sí o No)	Fuera de banda: ¿es necesario reiniciar el sistema?	En banda: ¿es necesario reiniciar el sistema?	Interfaz gráfica de usuario de Lifecycle Controller: ¿es necesario reiniciar?
	Diagnóstico	No	No	No	No
	Driver Pack del sistema operativo	No	No	No	No
	Lifecycle Controller	No	No	No	Sí
	BIOS	Sí	Sí	Sí	Sí
	Controladora RAID	Sí	Sí	Sí	Sí
	Planos posteriores	Sí	Sí	Sí	Sí
	Gabinetes	Sí	Sí	No	Sí
	NIC	Sí	Sí	Sí	Sí
	iDRAC	Sí	**No	*No	*No
	Unidad de fuente de alimentación	Sí	Sí	Sí	Sí
	CPLD	No	Sí	Sí	Sí
	Tarjetas de FC	Sí	Sí	Sí	Sí
	SSD PCIe	Sí	Sí	Sí	Sí

* Indica que si bien no es necesario reiniciar el sistema, se debe reiniciar la iDRAC para aplicar las actualizaciones. Se interrumpirán temporalmente la comunicación y la supervisión de la iDRAC.

** Cuando se actualiza iDRAC de la versión 1.30.30 o posterior, no es necesario reiniciar el sistema. Sin embargo, las versiones de firmware del iDRAC anteriores a la 1.30.30 requieren un reinicio del sistema cuando se aplican mediante las interfaces fuera de banda.

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

Todas las actualizaciones de componentes de LC entran en vigencia inmediatamente. Sin embargo, a veces los servicios del sistema pueden retrasar su aplicación. En tales casos, la actualización falla porque no está disponible el recurso compartido remoto que se aloja en la CMC.

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

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

1. En la interfaz web de la CMC, en el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.
   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**. Para obtener más información, consulte la sección Elección de tipo de actualización de 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 Filtrado de componentes para actualizaciones de firmware mediante la interfaz web del CMC.
4. En la columna **Update (Actualizar)**, seleccione las casillas de verificación de los componentes o dispositivos cuyo firmware desee actualizar con la próxima versión. Use el acceso directo de la tecla CTRL para seleccionar un tipo de componente o dispositivo y actualizarlo en todos los servidores aplicables. Si mantiene presionada la tecla CRTL, todos los componentes se resaltarán en amarillo. Mientras mantiene presionada la tecla CTRL, seleccione el componente o dispositivo que desee marcando la casilla de verificación asociada en la columna **Update (Actualizar)**.

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

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

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

5. Especifique el archivo de imagen del firmware para los componentes o dispositivos seleccionados. Este es un archivo de Dell Update Package (DUP) para Microsoft Windows.
6. Seleccione una de las siguientes opciones:
   - **Reiniciar ahora**: se reinicia el servidor y se aplica la actualización de firmware inmediatamente.
   - **En el siguiente reinicio**: se reinicia el servidor de forma manual en otro momento. La actualización de firmware se aplica después del siguiente reinicio.

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

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

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

La actualización de componentes de servidores desde un recurso compartido de red mediante Dell Repository Manager y la integración de chasis modular Dell PowerEdge M1000e simplifica la actualización, al emplear un firmware de paquete personalizado, para que pueda implementarlo de manera más fácil y rápida. Actualizar desde un recurso compartido de red proporciona flexibilidad para la actualización de todos los componentes del servidor de 12a generación al mismo tiempo con un mismo catálogo, desde un NFS o CIFS.

Este método ofrece una forma rápida y fácil de crear un repositorio personalizado para los sistemas conectados mediante Dell Repository Manager y el archivo de inventario del chasis exportado mediante la interfaz web de la CMC. DRM le permite crear un repositorio totalmente personalizado que solo incluye los paquetes de actualización para la configuración específica del sistema. También puede crear repositorios que contengan actualizaciones solo para dispositivos desactualizados, o un repositorio básico que contenga las 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 ubicación del recurso compartido. Mediante la interfaz web de la CMC, puede realizar la actualización de los componentes de uno o varios servidores.

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

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

- Los servidores deben pertenecer a la 12.ª generación o a generaciones posteriores y debe tener la licencia de iDRAC Enterprise.

- La versión del CMC debe ser 4.5 o posterior.
- Lifecycle Controller debe estar activado en los servidores.
- La versión 1.50.50 o posterior del iDRAC debe estar disponible en los servidores de 12.ª generación.
- Dell Repository Manager 1.8 o posterior debe estar instalado en el sistema.
- Debe tener privilegios de administrador de lal CMC.

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

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

1. En la interfaz web de la CMC, en el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.
   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde recurso compartido de red**. Para obtener más información, consulte Elección de tipo de actualización de los componentes del servidor.
3. Haga clic en **Guardar 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 repositorio se almacena en el recurso compartido de CIFS o NFS configurado por la CMC. Para obtener información sobre la creación de un repositorio mediante Dell Repository Manager, consulte *Dell Repository Manager Data Center Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Data Center versión 1.8)* y *Dell Repository Manager Business Client Version 1.8 User's Guide (Guía del usuario de Dell Repository Manager Business Client versión 1.8),* disponibles en **dell.com/support/manuals**.
4. Si el recurso compartido de red no está conectado, configure el recurso compartido de red del chasis. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web del CMC.
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.
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.

Filtrado de componentes para actualizaciones de firmware

La información de todos los componentes y dispositivos de todos los servidores se recupera de una sola vez. Para administrar esta gran cantidad de información, Lifecycle Controller proporciona varios mecanismos de filtrado. 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.
- Filtrar los componentes y los dispositivos seleccionados automáticamente para limitar la categoría de un componente o un dispositivo en particular por tipos o modelos.

NOTA: La función de filtrado automático es importante al utilizar Dell Update Packages (DUP). La programación de la 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 reducir al mínimo las decisiones de selección que se toman después una selección inicial.

Ejemplos

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 de todos los servidores. Si el conjunto de servidores consta de una serie de modelos de servidores y se selecciona un servidor para la actualización del BIOS, la lógica de filtrado automático quita automáticamente todos los otros servidores que no coinciden con el modelo del servidor seleccionado. Esto garantiza que la imagen de actualización del firmware (DUP) del BIOS seleccionada sea compatible con el modelo de servidor correcto.

  En ocasiones, la imagen de actualización del firmware del BIOS puede ser compatible con varios modelos de servidor. Estas optimizaciones se omiten por si la compatibilidad deja de existir en el futuro.

- El filtrado 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 la misma manera, las imágenes de actualización del firmware (DUP) pueden estar disponibles en formularios optimizados en los que un solo DUP puede estar programado para actualizar varios tipos o modelos de dispositivos de una categoría determinada.

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

Para filtrar los dispositivos:

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.
   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**.
3. En la sección **Filtro para actualizar componentes y dispositivos**, seleccione una o varias de las siguientes opciones:
   - BIOS
   - iDRAC
   - Lifecycle Controller
   - Diagnósticos de 32 bits
   - Driver Pack del sistema operativo
   - Controladora de la red I/F
   - Controladora RAID

   En la sección **Firmware Inventory (Inventario de firmware)** se presentan solamente los componentes o dispositivos asociados de todos los servidores presentes en el chasis. Se trata de un filtro de paso, lo que significa que solo acepta componentes o dispositivos asociados con el filtro, y excluye a todos los demás.

   Una vez que aparece el conjunto de componentes y dispositivos filtrado en la sección de inventario, se puede seguir filtrando cuando se selecciona un componente o dispositivo para su actualización. Por ejemplo, si se selecciona el filtro BIOS, la sección de inventario muestra todos los servidores solo con su componente de BIOS. Si se selecciona un componente de BIOS de uno de los servidores, el inventario se filtra aún más para mostrar solamente los servidores del mismo nombre de modelo que el seleccionado.

   Si no se selecciona ningún filtro y se selecciona un componente o dispositivo para su actualización en la sección de inventario, el filtro relacionado con esa selección se activa automáticamente. Se pueden aplicar otros filtros cuando la sección de inventario muestra todos los servidores que coinciden con el componente seleccionado en cuanto al modelo, el tipo u otra forma de identidad. Por ejemplo, si se selecciona un componente de BIOS de uno de los servidores para su actualización, el filtro se configura en el BIOS automáticamente y la sección de inventario muestra los servidores que coinciden con el nombre de modelo del servidor seleccionado.

Filtrado de componentes para actualizaciones de firmware mediante RACADM

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

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

Para obtener más información, consulte Chassis Management Controller for Dell PowerEdge M1000e RACADM Comand Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Visualización del inventario de firmware

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

Visualización del inventario de firmware mediante la interfaz web del CMC

Para ver el inventario de firmware:

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. Vea los detalles del inventario de firmware en la sección **Component/Device Firmware Inventory (Inventario de firmware de componente/dispositivo)**. En la tabla se muestran:
   - Los servidores que actualmente no admiten el servicio de Lifecycle Controller se detallan como **No admitido**. Se ofrece un hipervínculo a una página alternativa donde es posible actualizar de forma directa únicamente el firmware de la iDRAC. Esta página solo admite la actualización de firmware del iDRAC y no de otro componente o dispositivo en el servidor. La actualización de firmware del iDRAC no depende del servicio de Lifecycle Controller.
   - Si el servidor aparece como **No listo**, eso indica que cuando se recuperó el inventario de firmware, el iDRAC del servidor aún se estaba inicializando. Espere hasta que la iDRAC esté completamente operativa y luego actualice la página para obtener el inventario de firmware nuevamente.
   - Si el inventario de los componentes y dispositivos no refleja lo instalado físicamente en el servidor, deberá invocar a Lifecycle Controller durante el proceso de inicio del servidor. Esto ayuda a actualizar la información de los dispositivos y los componentes internos, y le permite verificar qué componentes y dispositivos están instalados. 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, las utilidades de configuración del iDRAC iDRAC Configuration Utility (para iDRAC) o iDRAC Settings Utility (para iDRAC) proporcionan una opción a la que se puede obtener acceso mediante la consola de inicio:

     - En la consola de inicio de los servidores iDRAC, cuando aparezca el mensaje `Press <CTRL-E> for Remote Access Setup within 5 sec.`, pulse `<CTRL-E>`. A continuación, en la pantalla de configuración, active **Collect System Inventory on Restart (Recopilar el inventario del sistema en el reinicio)**.
     - En la consola de inicio de los servidores iDRAC, seleccione F2 para acceder a la configuración del sistema. En la pantalla de configuración, seleccione iDRAC Settings (Configuración de iDRAC) y, a continuación, seleccione System Services (USC) (Servicios del sistema, USC). En la pantalla de configuración, active **Collect System Inventory on Restart (Recopilar el inventario del sistema en el reinicio)**.
   - Se encuentran disponibles opciones para las diferentes operaciones de Lifecycle Controller, como Actualizar, Revertir, Reinstalar y Eliminación de trabajos. Solo se puede realizar un tipo de operación por vez. Los componentes y los dispositivos no admitidos pueden 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 13. : Información sobre componentes y dispositivos

Campo	Descripción
Ranura	Muestra la ranura que ocupa el servidor en el chasis. Los números de ranura son Id. secuenciales, de 1 a 16 (para las 16 ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis. Si hay menos de 16 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, pase el mouse sobre la columna para ver la descripción. La descripción se muestra como en el ejemplo siguiente: `QLogic 577xx/578xx 10 Gb Ethernet BCM12345 - 22:X1:X2:X3:BB:0A`

Tabla 13. : Información sobre componentes y dispositivos (continuación)

Campo	Descripción
	NOTA: Los detalles de WWN de 16 tarjetas FC no aparecen en la sección **Inventario de firmware**.
Versión actual	Muestra la versión actual del componente o del dispositivo en el servidor.
Versión de reversión	Muestra la versión de reversión del componente o del dispositivo en el servidor.
Estado del trabajo	Muestra el estado del trabajo de las operaciones programadas en el servidor. El estado del trabajo se actualiza de forma dinámica permanentemente. Si se detecta por el estado que se completó un trabajo, las versiones del firmware de los componentes y los dispositivos en ese servidor se actualizan automáticamente, por si hubo algún cambio. También se muestra un icono de información junto al estado actual, para ofrecer información adicional sobre el estado actual del trabajo. Al hacer clic en el icono o mover el cursor por encima, se puede ver dicha información.
Actualizar	Selecciona el componente o el dispositivo para una actualización de firmware en el servidor.

Visualización del inventario de firmware mediante RACADM

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

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

Para obtener más información, consulte Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

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

Para guardar el informe de inventario del chasis:

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.
   Aparecerá la página **Actualización de los componentes del servidor**.
2. Haga clic en **Guardar 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. Debe tener la opción CSIOR activada en los servidores individuales y debe guardar el informe de inventario del chasis cada vez que se produzca un cambio en la configuración de hardware y software del chasis.

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

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

1. En la interfaz web de la CMC, en el árbol del sistema, vaya a **Server Overview (Descripción general del servidor)** y haga clic en **Network Share (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 introducir el nuevo nombre en este campo.

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

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

3. Haga clic en **Probar directorio** para verificar si se puede leer y escribir en los directorios.
4. Haga clic en **Probar conexión de red** para verificar si se puede acceder a la ubicación del recurso compartido de red.
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 configuración de un recurso compartido de red anterior.

Operaciones de Lifecycle Controller

Es posible realizar operaciones de Lifecycle Controller tales como:

- Vuelva a instalarla
- Revertir
- Actualizar
- Eliminar trabajos

Solo se puede realizar un tipo de operación por vez. Los componentes y los dispositivos no admitidos pueden 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: privilegio para Configurar el iDRAC y privilegio de Inicio de sesión en el iDRAC.

Una 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 la instalación del firmware, que también incluye una fase de verificación del firmware. Puede ver el progreso de este proceso con la consola del servidor. Si necesita actualizar varios componentes o dispositivos de un servidor, puede consolidar todas las actualizaciones en una operación programada y así reducir la cantidad de reinicios necesarios.

En ocasiones, cuando una operación está en proceso de enviarse para su programación a través de otra sesión o contexto, se intenta realizar otra operación. En ese caso, aparece un mensaje de confirmación para explicar la situación e indicar que la operación no debe enviarse. Espere a que la operación en curso se complete y luego vuelva a enviar la operación.

No salga de la página tras enviar una operación para su programación. Si lo intenta, aparece un mensaje de confirmación para permitirle cancelar. De lo contrario, la operación se interrumpe. Una interrupción, en especial durante la operación de actualización, puede poner fin a la carga del archivo de imagen del firmware antes de que se complete. Después de enviar una operación para su programación, asegúrese de aceptar el mensaje de confirmación que indica que la operación se ha programado correctamente.

Conceptos relacionados

Reinstalación del firmware de los componentes del servidor en la página 64
Reversión del firmware de los componentes del servidor en la página 65
Actualización de firmware de los componentes del servidor en la página 57
Eliminación de trabajos programados sobre el firmware de los componentes del servidor en la página 65

Reinstalación del firmware de los componentes del servidor

Puede reinstalar la imagen de firmware del firmware instalado actualmente 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 del servidor:

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. Filtre el componente o el dispositivo (opcional).
3. En la columna **Versión actual**, seleccione la casilla de verificación del componente o dispositivo para el cual desea volver a instalar el firmware.
4. Seleccione una de las siguientes opciones:
   - **Reiniciar ahora**: se reinicia el servidor
   - **En el siguiente reinicio**: se reinicia el servidor de forma manual en otro momento.
5. Haga clic en **Reinstall (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 previamente para 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.

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

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

1. En la interfaz web del CMC, expanda el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.
   Aparece la página **Actualización de componentes del servidor**; en la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**.
2. Filtre el componente o el dispositivo (opcional).
3. En la columna **Revertir versión**, active la casilla de verificación del componente o dispositivo para el cual desea revertir el firmware.
4. Seleccione una de las siguientes opciones:
   - **Reiniciar ahora**: se reinicia el servidor
   - **En el siguiente reinicio**: se reinicia el servidor de forma manual en otro momento.
5. Haga clic en **Rollback (Revertir)**. La versión del firmware instalada previamente se vuelve a instalar para el componente o dispositivo seleccionado.

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

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 la interfaz web del CMC, en el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Actualizar** > **Actualización de los componentes del servidor**.
   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**. Para obtener más información, consulte la sección Elección de tipo de actualización de los componentes del servidor.

   NOTA: No se puede realizar una operación de eliminación de trabajos en el modo **Actualizar desde recurso compartido de red** de la actualización de componentes de un servidor.

3. En la sección **Filtro para actualizar componentes y dispositivos**, filtre el componente o el dispositivo (opcional). Para obtener más información, consulte Filtrado de componentes para actualizaciones de firmware mediante la interfaz web del CMC.
4. En la columna **Job Status (Estado de trabajo)**, una marca junto al estado del trabajo indica que existe un trabajo de Lifecycle Controller en curso y que se encuentra en el estado indicado. Puede seleccionar el trabajo para una operación de eliminación.

5. Haga clic en **Eliminación de trabajos**.
   Se borran los trabajos para los componentes o dispositivos seleccionados.

Recuperación de firmware del iDRAC mediante el CMC

El firmware de la iDRAC se actualiza normalmente mediante interfaces de la iDRAC, como la interfaz web de la iDRAC, la interfaz de línea de comandos SM-CLP o los paquetes de actualización específicos del sistema operativo descargados de **support.dell.com**. Para obtener más información, consulte la Guía del usuario del iDRAC.

Las generaciones tempranas de servidores pueden recuperar el firmware dañado mediante el nuevo proceso de actualización de firmware de la iDRAC. Cuando la CMC detecta que el firmware de la iDRAC está dañado, presenta el servidor en la página **Firmware Update (Actualización del firmware)**. Siga los pasos que se indiquen para actualizar el firmware.

5

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

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

- CMC activos y en espera
- Todos los servidores y los servidores individuales
- Matrices de almacenamiento
- Todos los módulos de E/S y los módulos de E/S individuales
- Ventiladores
- iKVM
- Suministros de energía (PSU)
- Sensores de temperatura
- El conjunto de LCD

Temas:

Visualización de los resúmenes de los componentes del chasis

Al iniciar sesión en la interfaz web de la CMC, la página **Chassis Health (Condición del chasis)** le permite ver la condición del chasis y de sus componentes. Se ofrece una vista gráfica actual del chasis y sus componentes. Se actualiza de forma dinámica, y las superposiciones y los textos de los subgráficos se modifican automáticamente para reflejar el estado actual.

Ilustración 6. Ejemplo de gráficos de chasis en la interfaz web

Para ver la condición del chasis, vaya a **Chassis Overview (Descripción general del chasis)** > **Properties (Propiedades)** > **Health (Condición)**. Se presenta la condición general del chasis, las CMC activas y en espera, los módulos de servidor, los módulos de E/S, los ventiladores, el iKVM, los suministros de energía (PSU), los sensores de temperatura y el conjunto de LCD. Al hacer clic en cada componente, se muestra información detallada sobre ese componente. Además, se muestran los sucesos más recientes en el registro de hardware de la CMC. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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

Gráficos del chasis

El chasis se representa con las vistas frontal y posterior (las imágenes superior e inferior, respectivamente). Los servidores y la pantalla LCD se muestran en la vista frontal, mientras que los demás componentes se muestran en la vista posterior. La selección de los componentes está indicada en azul y se controla al hacer clic en la imagen del componente que se desee. Cuando un componente está presente en el chasis, el icono de ese tipo de componente se muestra en el gráfico en la posición (la ranura) donde está instalado. Las posiciones vacías se muestran con un fondo gris. El icono del componente indica visualmente su estado. Otros componentes muestran iconos que representan visualmente el componente físico. Los iconos de los servidores y los módulos de E/S abarcan varias ranuras cuando se instala un componente de doble tamaño. Al pasar el cursor sobre un componente aparece información adicional sobre ese componente.

Tabla 14. : Estados del icono del servidor

Icono	Descripción
	El servidor está encendido y funciona normalmente.
	El servidor está apagado.

Tabla 14. : Estados del icono del servidor (continuación)

Icono	Descripción
	El servidor indica un error no crítico.
	El servidor indica un error crítico.
	No hay servidores presentes.

Información del componente seleccionado

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

- Condición, rendimiento y propiedades: muestra los sucesos 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.
- Quick Links (Vínculos de acceso rápido): Ofrece vínculos para ir a las páginas más visitadas y también las acciones más realizadas. En esta sección solo se muestran vínculos aplicables al componente seleccionado.

NOTA: En Multi-Chassis Management (MCM) (Administración de varios chasis, MCM), no se muestran todos los **Quick Links (Vínculos de acceso rápido)** asociados con los servidores.

Tabla 15. Página Estado del chasis: propiedades de los componentes

Componente	Propiedades de condición y rendimiento	Propiedades	Vínculos de acceso rápido
Conjunto de LCD	• Condición de LCD • Condición del chasis	Ninguno	Ninguno
CMC activas y en espera	• Modo de redundancia • Dirección MAC • IPv4 • IPv6	• Firmware • Firmware en espera • Última actualización • Hardware	• Estado de la CMC • Sistema de red • Actualización del firmware
Todos los servidores y servidores individuales	• Estado de la alimentación • Consumo de energía • Condición • Energía asignada	• Nombre • Modelo • Etiqueta de servicio • Nombre del host	• Server Status (Estado del servidor) • Iniciar la consola remota • Iniciar la interfaz gráfica de usuario del iDRAC

Tabla 15. Página Estado del chasis: propiedades de los componentes (continuación)

Componente	Propiedades de condición y rendimiento	Propiedades	Vínculos de acceso rápido
	• Temperatura	• iDRAC • CPLD • BIOS • Sistema operativo • Información de la CPU • Memoria total del sistema	• Iniciar la interfaz gráfica de usuario de OMSA • Apagar el servidor • Recurso compartido de archivos remotos • Implementar red del iDRAC • Actualización de componentes del servidor
iKVM	Consola de OSCAR	• Nombre • Número de pieza • Firmware • Hardware	• Estado de iKVM • Actualización del firmware
Unidades del sistema de alimentación	Estado de la alimentación	Capacidad	• Estado del suministro de energía • Consumo de alimentación • Presupuesto del sistema
Ventiladores	• Velocidad	• Umbral crítico inferior • Umbral crítico superior	• Estado de los ventiladores
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. Expansión de los servidores en el árbol del sistema. Todos los servidores (de 1 a 16) aparecerán en la lista expandida Servidores. El nombre de una ranura sin servidor se mostrará atenuado.
2. Al pasar el cursor sobre el nombre o el número de ranura de un servidor, aparece información sobre herramientas con el nombre de modelo del servidor y la etiqueta de servicio (si está disponible).

Visualización del resumen del chasis

Es posible ver el resumen de los componentes instalados en el chasis.

Para ver la información del resumen del chasis, en la interfaz web del CMC, vaya a **Descripción general del chasis** > **Propiedades** > **Resumen**.
Aparecerá la página **Chassis Summary (Resumen del chasis)**. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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 del CMC, vaya a **Descripción general del chasis** > **Controladora del chasis** > **Propiedades** > **Estado**.
Aparecerá la página **Chassis Controller Status (Estado de la controladora del chasis)**. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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:

1. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   En la página **Chassis Health (Condición del chasis)** se ve una descripción gráfica de todos los servidores instalados en el chasis. La condición del servidor se indica mediante la superposición de un subgráfico. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
2. Vaya a **Descripción general del chasis** > **Descripción general del servidor** > **Propiedades** > **Estado**.
   La página **Servers Status (Estado de los servidores)** ofrece descripciones generales de los servidores del chasis. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización de información y estado de condición de un servidor individual

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

1. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   En la página **Chassis Health (Condición del chasis)** se ve una descripción gráfica de todos los servidores instalados en el chasis. La condición del servidor se indica mediante la superposición de un subgráfico. Mueva el cursor sobre el subgráfico de un servidor en particular. Así verá información adicional sobre el servidor. Haga clic en el subgráfico para ver la información de módulos de E/S a la derecha. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
2. Vaya a **Chassis Overview (Descripción general del chasis)** y expanda **Server Overview (Descripción general del servidor)** en el árbol del sistema. Todos los servidores (1 a 16) aparecerán en la lista expandida. Haga clic en el servidor (la ranura) que desee ver.
   En la página **Server Status (Estado del servidor)**, separada de la página **Servers Status (Estado de los servidores)**, se presenta la condición del servidor del chasis y un punto de inicio para la interfaz web de la iDRAC, que es el firmware utilizado para administrar el servidor. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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

Visualización de estado del arreglo de almacenamiento

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

1. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   En la página **Chassis Health (Condición del chasis)** se ve una descripción gráfica de todos los servidores instalados en el chasis. La condición del servidor se indica mediante la superposición de un subgráfico. Mueva el cursor sobre el subgráfico de un servidor en particular. Así verá información adicional sobre el servidor. Haga clic en el subgráfico para ver la información de módulos de E/S a la derecha. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
2. Vaya a **Chassis Overview (Descripción general del chasis)** y expanda **Server Overview (Descripción general del servidor)** en el árbol del sistema. Aparecerán todas las ranuras (1-16) en la lista expandida. Haga clic en la ranura donde se encuentra insertado el arreglo de almacenamiento.
   La página Storage Array Status (Estado del arreglo de almacenamiento) presenta la condición y las propiedades del arreglo de almacenamiento. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización de información y estado de condición de todos 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. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   Aparecerá la página **Estado del chasis**. La sección inferior de **Chassis Graphics (Gráficos del chasis)** ofrece la vista posterior del chasis y contiene información del estado de los módulos de E/S. Dicho estado se indica mediante la superposición del subgráfico del módulo. Mueva el cursor sobre el subgráfico de un módulo. El texto ofrece información adicional sobre el módulo. Haga clic en el subgráfico del módulo para ver la información a la derecha.
2. Vaya a **Descripción general del chasis** > **Descripción general del módulo de E/S** > **Propiedades** > **Estado**.
   La página **I/O Module Status (Estado de módulos de E/S)** proporciona descripciones generales de todos los módulos de E/S asociados con el chasis. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización de información y estado de condición de un módulo de E/S individual

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

1. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   Aparecerá la página **Estado del chasis**. La sección inferior de Chassis Graphics (Gráficos del chasis) ofrece la vista posterior del chasis y contiene información del estado de los módulos de E/S. Dicho estado se indica mediante la superposición del subgráfico del módulo. Mueva el cursor sobre el subgráfico de un módulo. El texto ofrece información adicional sobre el módulo. Haga clic en el subgráfico del módulo para ver la información a la derecha.
2. Diríjase a **Descripción general del chasis** y expanda **Descripción general del módulo de E/S** en el árbol del sistema. Aparecerán todos los módulos de E/S (1–6) en la lista expandida. Haga clic en el módulo de E/S (ranura) que desea ver S
   Aparecerá la página **I/O Module Status (Estado del módulo de E/S)** específica de la ranura del módulo de E/S (separada de la página general **I/O Module Status (Estado de módulos de E/S)**). Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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

Visualización de información y estado de condición de los ventiladores

La CMC, que controla la velocidad de los ventiladores, aumenta o disminuye automáticamente la velocidad en función de los sucesos que se producen en todo el sistema. 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 falla.
- Se desmonta un ventilador del chasis.

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

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

1. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   Aparecerá la página **Estado del chasis**. La sección inferior de los gráficos del chasis ofrece la vista posterior del chasis y contiene información del estado de los ventiladores. Dicho estado se indica mediante la superposición del subgráfico de los ventiladores. Mueva el cursor por el subgráfico de los ventiladores. El texto ofrece información adicional sobre los ventiladores. Haga clic en el subgráfico de los ventiladores para ver la información a la derecha.
2. Vaya a **Descripción general del chasis** > **Ventiladores** > **Propiedades**.
   La página **Fans Status (Estado de los ventiladores)** proporciona el estado y las mediciones de velocidad (en revoluciones por minuto o RPM) de los ventiladores del chasis. Puede haber uno o varios ventiladores.

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

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

Visualización de información y estado de condición del iKVM

El módulo KVM de acceso local para el chasis del servidor Dell M1000e se denomina módulo de conmutador KVM integrado Avocent o iKVM.

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

1. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   Aparecerá la página **Estado del chasis**. La sección inferior de los gráficos del chasis ofrece la vista posterior del chasis y contiene información del estado del iKVM. Dicho estado se indica mediante la superposición del subgráfico del iKVM. Al pasar el cursor sobre el subgráfico de un iKVM se muestra un texto. El texto ofrece información adicional sobre el iKVM. Haga clic en el subgráfico del iKVM para ver la información a la derecha.
2. Vaya a **Descripción general del chasis** > **iKVM** > **Propiedades**.
   La página **iKVM Status (Estado del IKVM)** muestra el estado y las lecturas del iKVM asociado con el chasis. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización de información y estado de condición de las unidades de suministro de energía

Para ver el estado de condición de las unidades de suministro de energía (PSU) asociadas con el chasis, realice alguno de los siguientes pasos:

1. Vaya a **Descripción general del chasis** > **Propiedades** > **Condición**.
   Aparecerá la página **Estado del chasis**. La sección inferior de los gráficos del chasis ofrece la vista posterior del chasis y contiene información del estado de todas las PSU. Dicho estado se indica mediante la superposición del subgráfico de la PSU. Al pasar el cursor sobre el subgráfico de una PSU se muestra un texto. El texto ofrece información adicional sobre la PSU. Haga clic en el subgráfico de la PSU para ver la información a la derecha.
2. Vaya a **Descripción general del chasis** > **Suministros de energía**.
   La página **Power Supply Status (Estado del suministro de energía)** muestra el estado y las lecturas de las PSU asociadas con el chasis. Allí se ve la condición general de la alimentación, el estado de la alimentación del sistema y el estado de redundancia de los suministros de energía. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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

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

Vaya a **Descripción general del chasis** > **Sensores de temperatura**.
La página **Temperature Sensors Status (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 *CMC Online Help (Ayuda en línea para el CMC)*.

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 del CMC excede el umbral, la velocidad de los ventiladores en el chasis aumenta.

Visualización de información y condición de la pantalla LCD

Para ver el estado de la condición de la pantalla LCD:

1. En la interfaz web del CMC, en el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Propiedades** > **Condición**.
   Aparecerá la página **Estado del chasis**. En la sección superior de los gráficos del chasis, se ilustra la vista frontal del chasis. El estado de la pantalla LCD se indica mediante la superposición del subgráfico de la pantalla LCD.
2. Mueva el cursor por el subgráfico de la pantalla LCD. Así verá información adicional sobre la pantalla LCD.
3. Haga clic en el subgráfico de la pantalla LCD para ver la información a la derecha. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

6

Configuración del CMC

El CMC permite configurar las propiedades del CMC, configurar usuarios y establecer alertas para realizar tareas de administración remotas.

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

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

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

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

- Si fuera necesario, modifique la configuración de la red.
- Configure las interfaces para obtener acceso al CMC.
- Configure la pantalla LED.
- Si fuera necesario, configure los grupos de chasis.
- Configure servidores, módulos de E/S o iKVM.
- 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.

Conceptos relacionados

Inicio de sesión en el CMC en la página 38
Visualización y modificación de la configuración de red LAN del CMC en la página 76
Configuración de las opciones de red y de seguridad de inicio de sesión del CMC en la página 79
Configuración de las propiedades de la etiqueta LAN virtual para CMC en la página 80
Configuración de servicios en la página 83
Configuración de los LED para identificar componentes en el chasis en la página 34
Configuración de un grupo de chasis en la página 85
Configuración del servidor en la página 105
Admin de fabric de entrada y salida en la página 184
Configuración y uso de iKVM en la página 196
Obtención de certificados en la página 90
Configuración de cuentas de usuario y privilegios en la página 131
Configuración del CMC para enviar alertas en la página 126
Admin y supervisión de la alimentación en la página 210
Configuración de varias CMC a través de RACADM mediante el archivo de configuración en la página 98

Temas:

- Configuración de varias CMC a través de RACADM mediante los perfiles de configuración de chasis
- Configuración de varias CMC a través de RACADM mediante el archivo de configuración
- Visualización y terminación de sesiones en el CMC
- Configuración de Modo de refrigeración mejorado para ventiladores

Visualización y modificación de la configuración de red LAN del CMC

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

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

Cuando IPv6 se activa en el momento del inicio, se envían tres solicitudes de enrutador cada cuatro segundos. Si los conmutadores de red externos ejecutan el protocolo de árbol de expansión (SPT), 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 requeridos.

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

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

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

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

1. En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **Network (Red)** > **Network (Red)**. En la página **Network Configuration (Configuración de la red)** se muestra la configuración actual de la red.
2. Modifique como desee la configuración general, de IPv4 o de IPv6. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
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

Utilice el comando `getconfig -g cfgcurrentlannetworking` para ver la configuración de IPv4.

Utilice el comando `getconfig -g cfgCurrentIPv6LanNetworking` para ver la configuración de IPv6.

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

Para obtener más información acerca de los objetos y subcomandos, consulte *Chassis Management Controller for PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

Activación de la interfaz de red del CMC

Para activar/desactivar la interfaz de red del 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/desactivar el direccionamiento IPv4 del 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/desactivar el direccionamiento IPv6 del 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.

De forma predeterminada, para IPv4, la CMC solicita y obtiene automáticamente en el servidor de protocolo de configuración dinámica de host (DHCP) una dirección IP para la CMC. Puede desactivar la función DHCP y especificar una dirección IP, una puerta de enlace y una máscara de subred estáticas para la CMC.

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

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

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

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

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

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

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

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

Activación o desactivación de DHCP para las direcciones IP de DNS

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

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

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

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

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

Establecimiento de direcciones IP estáticas de DNS

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

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

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

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

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

Configuración de valores de DNS para 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.

- **CMC Name (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.

- **DNS Domain Name (Nombre de dominio DNS)**: El nombre predeterminado del dominio DNS es un solo carácter en blanco. Para establecer un nombre de dominio DNS, escriba:

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSDomainName <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 viene 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 de la unidad de transmisión máxima para IPv4 e IPv6

La propiedad de unidad de transmisión máxima (MTU) le permite establecer un límite de tamaño para los paquetes transferidos mediante la interfaz. Para definir la MTU, escriba:

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

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

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

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

Las funciones de bloqueo de direcciones IP y de bloqueo de usuarios en la CMC le permiten prevenir problemas de seguridad provocados por intentos de adivinar contraseñas. Esta función le permite bloquear usuarios y un rango de direcciones IP que pueden acceder a la CMC. La función de bloqueo de direcciones IP viene activada en la CMC de forma predeterminada. Usted puede configurar los atributos del rango de IP mediante la interfaz web de la CMC o RACADM. Para usar las funciones de bloqueo de direcciones IP y de bloqueo de usuarios, active las opciones mediante la interfaz web de la CMC o RACADM. Configure las opciones de la política de bloqueo de inicio de sesión para establecer la cantidad de intentos de inicio de sesión incorrectos permitidos para un usuario o una dirección IP específicos. Una vez superado este límite, el usuario bloqueado podrá iniciar sesión solo después de transcurrido el tiempo de penalidad.

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

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

NOTA: Para realizar la siguiente tarea, debe tener privilegios de **Administrador de configuración del chasis**.

Para configurar los atributos de rango de IP con la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **Network (Red)** > **Network (Red)**. Aparecerá la página **Configuración de red**.
2. En la sección Configuración de IPv4, haga clic en **Opciones avanzadas**.
   Aparecerá la página **Seguridad de inicio de sesión**.

   Otra manera de acceder a la página Log in Security (Seguridad de inicio de sesión) es ir en el árbol del sistema a **Chassis Overview (Descripción general del chasis)** y hacer clic en **Security (Seguridad)** > **Log in (Inicio de sesión)**.
3. Para activar la función de verificación de rango de IP, en la sección **Rango de IP**, seleccione la opción **Rango de IP activado**.
   Se activarán los campos **Dirección de rango de IP** y **Máscara de rango de IP**.
4. En los campos **Dirección de rango de IP** y **Máscara de rango de IP**, escriba el rango de direcciones IP y de máscaras de rangos de IP para los que desea bloquear el acceso al CMC.

   Para obtener más información, consulte *CMC Online Help (Ayuda en línea de la CMC)*.
5. Haga clic en **Aplicar** para guardar la configuración.

Configuración de los atributos de rango de IP con RACADM

Puede configurar los siguientes atributos de rango de IP para el CMC con RACADM:

- Función de verificación de rango de IP
- Rango de direcciones IP para las que desea bloquear el acceso al CMC
- Máscara del rango de IP para el que desea bloquear el acceso al CMC

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP especificado. Solo se autoriza un inicio de sesión de una dirección IP entrante si los dos valores siguientes son idénticos:

- **cfgRacTuneIpRangeMask** en cantidad de bits y con la dirección IP entrante
- **cfgRacTuneIpRangeMask** en cantidad de bits y con **cfgRacTuneIpRangeAddr**
- Para activar la función de verificación de rango de IP, use la siguiente propiedad en el grupo `cfgRacTuning`:

  ```
  cfgRacTuneIpRangeEnable <0/1>
  ```
- Para especificar el rango de direcciones IP para las que desea bloquear el acceso a la CMC, use la siguiente propiedad en el grupo `cfgRacTuning` :

  ```
  cfgRacTuneIpRangeAddr
  ```
- Para especificar la máscara del rango de IP para la que desea bloquear el acceso a la CMC, use la siguiente propiedad en el grupo `cfgRacTuning` :

  ```
  cfgRacTuneIpRangeMask
  ```

Configuración de las propiedades de la etiqueta LAN virtual para CMC

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.

Configuración de las propiedades de la etiqueta LAN virtual para CMC mediante la interfaz web

Para configurar la red VLAN para CMC mediante la interfaz web del CMC:

1. Desplácese a cualquiera de las siguientes páginas:
   - En el árbol del sistema, diríjase a **Descripción general del chasis** y haga clic en **Red** > **VLAN**.
   - En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** > **Server Overview (Descripción general del servidor)** y haga clic en **Network (Red)** > **VLAN**.

   Aparecerá la página **Configuración de la etiqueta VLAN**. Las etiquetas VLAN son propiedades del chasis. Se conservan en el chasis aunque se elimine un componente.
2. En la sección **CMC**, active la VLAN para la CMC, establezca la prioridad y asigne la Id. Para obtener más información acerca de los campos, consulte *CMC Online Help (Ayuda en línea de la CMC)*.
3. Haga clic en **Aplicar**. Se guardará la configuración de la etiqueta VLAN.

   También puede obtener acceso a esta página a través de **Descripción general del chasis** > **Servidores** > **Configuración** > **VLAN** subficha.

Configuración de las propiedades de la etiqueta LAN virtual para CMC mediante RACADM

1. Active las capacidades de VLAN de la red de administración del chasis externo:

   ```
   racadm config -g cfgLanNetworking -o
   cfgNicVLanEnable 1
   ```
2. Especifique la identificación de VLAN para la red de administración del chasis externo:

   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
   ```

   Los valores válidos para `<VLAN id>` son 1-4000 y 4021-4094. El valor predeterminado es 1.

   Por ejemplo:

   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID
   1
   ```
3. A continuación, especifique la prioridad de VLAN para la red de administración del chasis externo:

   ```
   racadm config -g cfgLanNetworking -o
   cfgNicVLanPriority <VLAN priority>
   ```

   Los valores válidos para `<VLAN priority>` son 0-7. El valor predeterminado es 0.

   Por ejemplo:

   ```
   racadm config -g cfgLanNetworking -o
   cfgNicVLanPriority 7
   ```

   También puede especificar la identificación y la prioridad de VLAN con un solo comando:

   ```
   racadm setniccfg -v <VLAN id> <VLAN priority>
   ```

   Por ejemplo:

   ```
   racadm setniccfg -v 1 7
   ```

4. Para eliminar la VLAN del CMC, desactive las capacidades de VLAN de la red de administración del chasis externo:

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

También puede eliminar la VLAN del CMC con el siguiente comando:

```
racadm setniccfg -v
```

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 del CMC: permita el acceso al CMC mediante la consola serie.
- Servidor web: Permita el acceso a la interfaz web de la CMC. Si desactiva la opción, utilice RACADM local para volver a activar el servidor web, ya que al desactivar el servidor web también desactiva RACADM remoto.
- SSH: permita el acceso a la CMC mediante la funcionalidad RACADM de firmware.
- Telnet: permita el acceso a la CMC mediante la funcionalidad RACADM de firmware.
- RACADM: permita el acceso al CMC mediante la funcionalidad RACADM.
- SNMP: active la CMC para enviar capturas SNMP para los sucesos.
- Syslog remoto: active el CMC para registrar sucesos en un servidor remoto.

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

El 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 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 suele producirse como consecuencia de alguno de los siguientes sucesos:

- La configuración de red o las propiedades de seguridad de la red se modificaron a través de la interfaz de usuario web del CMC o RACADM.
- La configuración del puerto de Web Server se modificó a través de la interfaz de usuario web o RACADM.
- Se restablece la CMC.
- Se carga un nuevo certificado del servidor SSL.

NOTA: Para modificar la configuración de los servicios, es necesario contar con 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 entrada de registro generada por la CMC se reenvía a los destinos.

NOTA: Puesto que el transporte de red para las anotaciones de registro reenviadas es UDP, no se garantiza que las anotaciones de registro se entreguen ni que el CMC reciba comentarios para indicar si las anotaciones se recibieron correctamente.

Configuración de los servicios mediante la interfaz web del CMC

Para configurar los servicios del CMC mediante la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Chassis Overview (Descripción general del chasis)** y luego haga clic en **Network (Red)** > **Services (Servicios)**. Aparecerá la página **Servicios de directorio**.
2. Configure los servicios siguientes según sea necesario:
   - Consola serie del CMC
   - Web Server

- SSH
- Telnet
- RACADM remoto
- SNMP
- Syslog remoto

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

3. Haga clic en **Aplicar** y actualice todos los intervalos de tiempo de espera predeterminados y los límites máximos de tiempo de espera.

Configuración de servicios mediante RACADM

Para activar y configurar los distintos servicios, utilice los siguientes objetos RACADM:

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Para obtener más información acerca de estos objetos, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Si el firmware del servidor no admite una función, al configurar una propiedad relacionada con esa función se genera un error. Por ejemplo, si se utiliza RACADM para activar el syslog remoto en una iDRAC no compatible, aparecerá un mensaje de error.

De forma similar, al mostrar las propiedades del iDRAC mediante el comando getconfig de RACADM, los valores de las propiedades aparecerán como N/A para una función no admitida en el servidor.

Por ejemplo:

```
$ racadm getconfig -g cfgSessionManagement -m server-1
# cfgSsnMgtWebServerMaxSessions=N/A
# cfgSsnMgtWebServerActiveSessions=N/A
# cfgSsnMgtWebServerTimeout=N/A
# cfgSsnMgtSSHMaxSessions=N/A
# cfgSsnMgtSSHActiveSessions=N/A
# cfgSsnMgtSSHTimeout=N/A
# cfgSsnMgtTelnetMaxSessions=N/A
# cfgSsnMgtTelnetActiveSessions=N/A
# cfgSsnMgtTelnetTimeout=N/A
```

Configuración de la tarjeta de almacenamiento extendido del CMC

Puede activar o reparar los medios flash extraíbles opcionales para utilizarlos como almacenamiento extendido no volátil. Algunas funciones de la CMC necesitan almacenamiento extendido no volátil.

Para activar o reparar los medios flash extraíbles mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y, a continuación, haga clic en **Chassis Controller (Controladora del chasis)** > **Flash Media (Medios flash)**. Aparecerá la página Removable Flash Media (Medios flash extraíbles).
2. En el menú desplegable, seleccione una de las opciones siguientes según sea necesario:
   - Usar los medios flash para almacenar datos del chasis
   - Reparar medios del controlador activo
   - Comenzar la replicación de datos entre medios
   - Detener la replicación de datos entre medios
   - Detener el uso de los medios flash para almacenar datos del chasis

   Para obtener más información sobre estas opciones, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
3. Haga clic en **Aplicar** para aplicar la opción seleccionada.

   Si existen dos CMC en el chasis, ambas deben contener un medio flash. Las funciones de la CMC que necesitan medios flash (excepto Flexaddress) no funcionan correctamente hasta que se instale y se active en esta página un medio autorizado por Dell.

Configuración de un grupo de chasis

La CMC le permite supervisar varios chasis desde un mismo 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.

Las funciones del grupo de chasis son las siguientes:

- La página **Grupo de chasis** muestra imágenes de la parte frontal y posterior de cada chasis. Hay un grupo de imágenes que corresponde al chasis principal y un grupo más por cada elemento del grupo.
- Los problemas en la condición del chasis principal y de los miembros de un grupo se marcan en rojo o amarillo y con una X o un ! en el componente que muestra los síntomas. Los detalles se muestran debajo de la imagen del chasis al hacer clic en la imagen o en **Details (Detalles)**.
- Los vínculos de inicio rápido están disponibles para abrir las páginas web del servidor o del chasis miembro.
- Hay un componente blade 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 ocho miembros. Además, cada chasis principal o miembro solo puede participar en un grupo. No se puede agregar a un grupo un chasis, ya sea como principal o miembro, que ya forme parte de otro grupo. Puede eliminar el chasis de un grupo y agregarlo luego a otro grupo.

Para configurar el grupo de chasis mediante la interfaz web del CMC:

1. Inicie sesión con privilegios de administrador de chasis en el chasis que planea configurar como principal.
2. Haga clic en **Configuración** > **Administración de grupos**. Aparecerá la página **Chassis Group (Grupo de chasis)**.
3. En la página **Chassis Group (Grupo de chasis)**, en **Role (Rol)**, seleccione **Leader (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 un grupo de chasis, la GUI pasa automáticamente a la página **Chassis Group (Grupo de chasis)**. El árbol del sistema presenta el grupo con su nombre, y el chasis principal y el chasis miembro desocupado aparecen en el árbol del sistema.

   NOTA: Asegúrese de que la versión del chasis principal siempre sea la más reciente.

Tareas relacionadas

Adición de miembros a un grupo de chasis en la página 85
Eliminación de un miembro del chasis principal en la página 86
Forma de desmontar un grupo de chasis en la página 86
Desactivación de un miembro del chasis miembro en la página 86
Inicio de la página web de un servidor o de un chasis miembro en la página 86
Propagación de las propiedades del chasis principal al chasis miembro en la página 87

Adición de miembros a un grupo de chasis

Una vez configurado el grupo de chasis, puede agregar miembros al grupo:

1. Inicie sesión en el chasis principal con los privilegios de administrador de chasis.
2. Seleccione el chasis principal en el árbol.
3. Haga clic en **Configuración** > **Administración de grupos**.
4. En **Administración de grupos**, introduzca el nombre de DNS o la dirección IP del miembro en el campo **Nombre del host/ Dirección IP**.

   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 de chasis en el chasis miembro.
6. Introduzca la contraseña correspondiente en el campo **Contraseña**.
7. Haga clic en **Aplicar**.

8. Repita del paso 4 al 8 para agregar un máximo de ocho miembros. Los nombres de chasis de los miembros nuevos aparecen en el cuadro de diálogo **Members (Miembros)**.

   Al seleccionar el grupo en el árbol se muestra el estado del miembro nuevo. Si hace clic en la imagen del chasis o el botón de detalles, podrá ver la información detallada.

   NOTA: Las credenciales introducidas para un miembro se pasan de forma segura al chasis miembro, para establecer una relación de confianza entre el chasis miembro y el principal. Las credenciales no se conservan en ningún chasis y nunca se intercambian nuevamente después de establecerse la relación de confianza inicial.

   Para obtener información sobre la propagación de las propiedades del chasis principal a los chasis miembro, consulte Propagación de las propiedades del chasis principal al chasis miembro.

Eliminación de un miembro del chasis principal

Puede 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. Seleccione el chasis principal en el árbol.
3. Haga clic en **Configuración** > **Administración de grupos**.
4. En la lista **Eliminar miembros**, seleccione el nombre o los nombres de los miembros que desea eliminar y, a continuación, haga clic en **Aplicar**.

   El chasis principal luego se comunicará con el miembro o los miembros que se hayan eliminado del grupo. Se eliminarán los nombres de los miembros. Si no se logra el contacto entre un chasis miembro y el principal debido a un problema en la red, es posible que el chasis miembro no reciba el mensaje. En ese caso, desactive el miembro desde el chasis miembro para completar la eliminación.

Tareas relacionadas

Desactivación de un miembro del chasis miembro en la página 86

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 árbol.
3. Haga clic en **Configuración** > **Administración de grupos**.
4. En la página **Grupo de chasis**, en **Función**, seleccione **Ninguno** y, a continuación, haga clic en **Aplicar**.

   El chasis principal luego comunica a todos los miembros que han sido eliminados del grupo. Por último, el chasis principal finalizará su función. Ahora es posible nombrarlo chasis miembro o principal de otro grupo.

   Si no se logra el contacto entre un chasis miembro y el principal debido a un problema en la red, es posible que el chasis miembro no reciba el mensaje. En ese caso, desactive el miembro desde el chasis miembro para completar la eliminación.

Desactivación de un miembro del chasis miembro

En ocasiones, el chasis principal no puede quitar un miembro de un grupo. Esto sucede si se pierde la conectividad de red con el miembro. Para eliminar un miembro de un grupo desde el chasis miembro:

1. Inicie sesión en el chasis miembro con privilegios de administrador.
2. Haga clic en **Configuración** > **Administración de grupos**.
3. Seleccione **Ninguno** y, a continuación, haga clic en **Aplicar**.

Inicio de la página web de un servidor o de un chasis miembro

Los vínculos de la página web de un chasis miembro, la consola remota de un servidor o la pagina web de la iDRAC del servidor dentro del grupo se encuentran disponibles en la página del grupo del chasis principal. Para iniciar sesión en el dispositivo miembro, puede utilizar el nombre de usuario y la contraseña con los que inició sesión en el chasis principal. Si el dispositivo miembro tiene las mismas credenciales de inicio de sesión, no es necesario un inicio de sesión adicional. De lo contrario, se dirige al usuario a la página de inicio de sesión del dispositivo miembro.

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 **Launch CMC (Iniciar CMC)** cuando los dos chasis, principal y miembro, tienen activado o desactivado FIPS, se lo dirigirá a la página **Chassis Group Health (Condición del grupo de chasis)**. De lo contrario, se lo dirigirá a la página **Login (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. Seleccione el servidor en la imagen del chasis que aparece debajo del panel **Health and Alerts (Condición y alertas)**.
   c. En el cuadro **Quick Links (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, todos los **Quick Links (Vínculos de acceso rápido)** asociados con los servidores no se muestran.

Propagación de las propiedades del chasis principal al chasis miembro

Puede aplicar las propiedades del chasis principal en el 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:
   - On-Change Propagation (Propagación ante cambio): Seleccione esta opción para propagar automáticamente los valores seleccionados de la configuración de propiedades del chasis. Las propiedades se propagan a todos los miembros actuales del grupo cada vez que se hacen cambios en el chasis principal.
   - Manual Propagation (Propagación manual): Seleccione esta opción para propagar manualmente a los miembros las propiedades del chasis principal del grupo. La configuración de propiedades del chasis principal se propaga a los miembros del grupo solo cuando el administrador del chasis principal hace clic en **Propagate (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 sean idénticas en todos los miembros del grupo de chasis. Por ejemplo, seleccione la categoría **Logging and Alerting Properties (Propiedades de registro y alerta)** para permitir que todos los chasis del grupo tengan 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 *CMC Online Help (Ayuda en línea de la CMC)*.

Inventario del servidor para el grupo de administración de múltiples chasis

En la página Chassis Group Health (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 navegador. El informe contiene datos de:

- Todos los servidores presentes actualmente en todos los chasis del grupo (incluido el principal).
- Las ranuras vacías y las ranuras de extensión (incluidas las instancias de servidores de altura completa y de doble ancho).

Forma de guardar el informe de inventario del servidor

Para guardar el informe de inventario del servidor mediante la interfaz web del CMC:

1. En el árbol del sistema, seleccione el **Grupo**.

Aparecerá la página **Condición del grupo de chasis**.

2. 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 servidor.

   NOTA: El principal del grupo de chasis, el chasis miembro y los servidores en el chasis asociado deben estar **Activados** para obtener el informe de inventario del servidor más preciso.

Datos exportados

El informe de inventario del servidor contiene los datos más recientes que cada miembro del grupo de chasis ha devuelto durante el sondeo normal del líder del grupo de chasis (una vez cada 30 segundos).

Para obtener el informe de inventario del servidor más preciso posible:

- El chasis principal y todos los chasis miembro del grupo se deben encontrar en **Estado de alimentación del chasis encendido**.
- Todos los servidores en el chasis asociado deben estar encendidos.

Es posible que el informe de inventario no incluya los datos de inventario para el chasis asociado y los servidores si un subconjunto del chasis miembro del grupo se encuentra:

- En **Estado de alimentación del chasis apagado**
- Apagado

NOTA: Si se inserta un servidor mientras el chasis está apagado, el número de modelo no se muestra en ningún lado en la interfaz web hasta que el chasis se vuelve a encender.

En la siguiente tabla se enumeran los campos de datos y los requisitos específicos para los campos que se deben incluir en el informe sobre cada servidor:

Campo de datos	Ejemplo
Nombre del chasis	Chasis principal del centro de datos
Dirección IP del chasis	192.168.0.1
Ubicación de ranura	1
Nombre de ranura	RANURA-01
Nombre del host	Servidor web corporativo **NOTA:** Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.
Sistema operativo	Microsoft Windows Server 2012, Standard x64 Edition **NOTA:** Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.
Modelo	PowerEdgeM630
Etiqueta de servicio	1PB8VF2
Memoria total del sistema	4.0 GB **NOTA:** Requiere CMC 5.0 (o posterior).
N.º de CPU	2 **NOTA:** Requiere CMC 5.0 (o posterior).

Información de CPU	Intel (R) Xeon (R) CPU E5-2690 v3@2,60 GHz

Formato de datos

El informe de inventario se genera en un formato de archivo `.CSV`, para que se pueda importar en diferentes herramientas, como Microsoft Excel. El archivo `.CSV` del informe de inventario se puede importar en la plantilla al seleccionar **Data (Datos)** > **From Text (Desde texto)** en MS Excel. Una vez que el informe de inventario se haya importado en MS Excel, si aparece un mensaje para solicitar información adicional, seleccione Comma-Delimited (Delimitado por comas) para importar el archivo en MS Excel.

Inventario del grupo de chasis y versión de firmware

La página **Chassis Group Firmware Version (Versión de firmware del grupo de chasis)** muestra el inventario de grupos y las versiones de firmware de los servidores y los componentes de servidores del chasis. Esta página también le permite organizar la información de inventario y filtrar la vista de las versiones de firmware. La vista mostrada se basa en los servidores o en cualquiera de los siguientes componentes de servidores del chasis:

- BIOS
- iDRAC
- CPLD
- USC
- Diagnóstico
- Controladores de SO
- RAID
- NIC

NOTA: La información de inventario mostrada en cuanto a grupo de chasis, chasis miembro, servidores y componentes de servidores se actualiza cada vez que se agrega o se elimina un chasis del grupo.

Visualización del inventario del grupo de chasis

Para ver el grupo de chasis mediante la interfaz web de la CMC, en el árbol del sistema, seleccione **Group (Grupo)**. Haga clic en **Properties (Propiedades)** > **Firmware Version (Versión de firmware)**. La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.

Visualización del inventario del chasis seleccionado con la interfaz web

Para ver el inventario del chasis seleccionado con la interfaz web del CMC:

1. En el árbol del sistema, seleccione **Group (Grupo)**. Haga clic en **Properties (Propiedades)** > **Firmware Version (Versión de firmware)**.
   La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.
2. En la sección **Seleccionar un chasis**, seleccione el chasis miembro del que desea ver el inventario.
   La sección **Filtro de visualización de firmware** muestra el inventario de servidor del chasis seleccionado y las versiones de firmware de todos los componentes del servidor.

Visualización de las versiones de firmware de los componentes de servidor seleccionados con la interfaz web

Para ver las versiones de firmware de los componentes de servidores seleccionados con la interfaz web del CMC:

1. En el árbol del sistema, seleccione **Group (Grupo)**. Haga clic en **Properties (Propiedades)** > **Firmware Version (Versión de firmware)**.
   La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.
2. En la sección **Seleccionar un chasis**, seleccione el chasis miembro del que desea ver el inventario.

3. En la sección **Filtro de visualización de firmware**, seleccione **Componentes**.
4. En la lista **Componentes**, seleccione el componente requerido (BIOS, iDRAC, CPLD, USC, Diagnóstico, unidad de SO, dispositivos RAID [hasta 2] y dispositivos NIC [hasta 6]) para los que desea ver la versión de firmware.
   Aparecerán las versiones de firmware del componente seleccionado de todos los servidores en el chasis miembro seleccionado.

   NOTA: Las versiones de firmware de USC, diagnóstico, unidad de SO, dispositivos RAID y dispositivos NIC de servidores no estarán disponibles en los siguientes casos:

   - El servidor pertenece a la 10a generación de servidores PowerEdge. Estos servidores no admiten Lifecycle Controller.
   - El servidor pertenece a la 11ma generación de servidores PowerEdge, pero el firmware de iDRAC no admite Lifecycle Controller.
   - La versión de firmware de la CMC de un chasis miembro es anterior a la versión 4.45. En este caso, los componentes de los servidores del chasis no aparecerán, aunque los servidores admitan Lifecycle Controller.

Obtención de certificados

En la tabla siguiente se enumeran los tipos de certificados basado en el tipo de inicio de sesión.

Tabla 16. Tipos de inicio de sesión y certificado

Tipo de inicio de sesión	Tipo de certificado	Cómo obtenerlo
Inicio de sesión único mediante Active Directory	Certificado de CA de confianza	Generar una CSR y hacer que la firme una autoridad de certificados
Inicio de sesión mediante tarjeta inteligente como usuario de Active Directory	• Certificado de usuario • Certificado de CA de confianza	• Certificado de usuario: exportar el certificado de usuario de tarjeta inteligente como un archivo de codificación Base64 mediante el software de administración de tarjetas suministrado por el proveedor de la tarjeta inteligente. • Certificado de CA de confianza: este certificado lo emite una CA.
Inicio de sesión de usuario de Active Directory	Certificado de CA de confianza	Este certificado lo emite una CA.
Inicio de sesión de usuario local	Certificado SSL	Generar una CSR y hacer que la firme una CA de confianza **NOTA:** La CMC viene con un certificado de servidor SSL autofirmado predeterminado. La consola virtual y el servidor web de la CMC utilizan este certificado.

Conceptos relacionados

Certificados de servidor de capa de sockets seguros en la página 90

Certificados de servidor de capa de sockets seguros

La CMC incluye un servidor web configurado para usar el protocolo de seguridad estándar de la industria Capa de sockets seguros (SSL) para transferir datos cifrados por Internet. SSL se basa en la tecnología de cifrado de claves públicas y privadas, y es una técnica muy popular para ofrecer comunicación cifrada y autentificada entre clientes y servidores, a fin de evitar el espionaje en las redes.

SSL permite que un sistema habilitado con SSL realice las siguientes tareas:

- Autentificarse ante un cliente habilitado con SSL
- Permitir que el cliente se autentifique ante el servidor
- Permitir que ambos sistemas establezcan una conexión cifrada

Este proceso de cifrado proporciona un alto nivel de protección para los datos. La CMC emplea la norma de cifrado SSL de 128 bits, la forma de cifrado más segura disponible para los navegadores de Internet en Norteamérica.

El servidor web de la CMC incluye un certificado digital SSL autofirmado de Dell (Id. de servidor). Para garantizar alta seguridad en Internet, sustituya el certificado SSL del servidor web enviando una solicitud a la CMC para generar una nueva solicitud de firma de certificado (CSR).

En el momento de reiniciar, se generará un nuevo certificado autofirmado en los siguientes casos:

- No existe un certificado personalizado presente
- No existe un certificado autofirmado presente
- El certificado autofirmado está dañado
- El certificado autofirmado ha vencido (dentro de un lapso de 30 días)

El certificado autofirmado presenta el nombre común <cmcname.domain-name>, donde cmcname es el nombre de host de la CMC y domain-name es el nombre del dominio. Si el nombre del dominio no está disponible, se muestra solo el nombre de dominio parcial (PQDN), que es el nombre de host de la CMC.

Solicitud de firma de certificado

Una solicitud de firma de certificado (CSR) es una solicitud digital a una autoridad de certificados (lo que se conoce como CA en la interfaz web) para obtener un certificado de servidor seguro. Los certificados de servidor seguro protegen la identidad de los sistemas remotos y garantizan que nadie pueda ver ni modificar la información que se intercambia con dichos sistemas. Para garantizar la seguridad de su CMC, se recomienda enfáticamente generar una CSR, enviarla a una autoridad de certificados y cargar el certificado recibido de la autoridad.

Una autoridad de certificados es una entidad comercial reconocida en la industria de TI por cumplir con altas normas de filtrado confiable, identificación y otro criterios de seguridad importantes. Algunas Autoridades de certificados son Thawte y VeriSign. Cuando en la autoridad se recibe su CSR, revisan y verifican la información incluida. Si el solicitante cumple con las normas de seguridad de la autoridad, se emite un certificado que identifica al solicitante de manera exclusiva para transacciones en redes y en Internet.

Una vez que la autoridad aprueba la CSR y le envía el certificado, usted debe cargarlo en el firmware de la CMC. La información de la CSR almacenada en el firmware de la CMC debe coincidir con la información incluida en el certificado.

NOTA: Para configurar los valores de SSL para el CMC, es necesario contar con privilegios de **Administrador de configuración del chasis**.

NOTA: Todos los certificados de servidor que se carguen deben estar vigentes (no deben haber expirado) y deben estar firmados por una autoridad de certificados.

Conceptos relacionados

Generación de una nueva solicitud de firma de certificado en la página 91
Carga del certificado del servidor en la página 92
Visualización del certificado del servidor en la página 93

Generación de una nueva solicitud de firma de certificado

Para garantizar la seguridad, se recomienda enfáticamente obtener y cargar en la CMC un certificado de servidor seguro. Los certificados de servidor seguro protegen la identidad de los sistemas remotos y garantizan que nadie pueda ver ni modificar la información que se intercambia con dichos sistemas. Sin un certificado de servidor seguro, la CMC es vulnerable al acceso de usuarios no autorizados.

Para obtener un certificado de servidor seguro para la CMC, debe enviar una solicitud de firma de certificado (CSR) a la autoridad de certificados que desee. Una CSR es una solicitud digital de un certificado de servidor seguro que contiene información sobre su organización y una clave de identificación exclusiva.

Después de generar una CSR, se le pedirá que guarde una copia en la estación de administración o en la red compartida, y la información exclusiva usada para generar la CSR se almacenará en la CMC. Esta información se utilizará posteriormente para autentificar el certificado de servidor que se reciba de la autoridad de certificados. Después de recibir el certificado de servidor de la autoridad de certificados, debe cargarlo en la CMC.

NOTA: Para que el CMC acepte el certificado de servidor emitido por la autoridad de certificados, la información de autentificación contenida en el nuevo certificado debe coincidir con la información almacenada en el CMC cuando se generó la CSR.

PRECAUCIÓN: Cuando se genera una CSR nueva, sobrescribe la CSR anterior en la CMC. Si una CSR pendiente se sobrescribe antes de que la autoridad de certificados otorgue el certificado, la CMC no aceptará el certificado porque la información que usa para autentificarlo se habrá perdido. Tenga cuidado al generar CSR, para no sobrescribir ninguna CSR pendiente.

Generación de una nueva solicitud de firma de certificado mediante la interfaz web

Para generar una solicitud de firma de certificado mediante la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Chassis Overview (Descripción general del chasis)** y luego haga clic en **Network (Red)** > **SSL**. Aparecerá **SSL Main Menu (Menú principal de SSL)**.
2. Seleccione **Generar una nueva solicitud de firma de certificado (CSR)** y haga clic en **Siguiente**. Aparece la página **Generar una nueva solicitud de firma de certificado (CSR)**.
3. Escriba un valor para cada atributo de la CSR.
4. Haga clic en **Generar**. Aparecerá el cuadro de diálogo **File Download (Descarga de archivo)**.
5. Guarde el archivo `csr.txt` en su estación de administración o red compartida. También puede abrir el archivo ahora y guardarlo después. Posteriormente, debe enviar este archivo a una autoridad de certificados.

Generación de CSR mediante RACADM

Para generar una CSR, utilice los objetos del grupo `cfgRacSecurityData` para especificar los valores y utilice el comando `sslcsrgen` para generar la CSR. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Carga del certificado del servidor

Después de generar una CSR, puede cargar el certificado del servidor SSL firmado en el firmware de la CMC. La CMC se restablece tras cargar el certificado. La CMC solo acepta certificados de servidor web X509 codificados en base 64.

PRECAUCIÓN: Durante el proceso de carga del certificado, el CMC no está disponible.

NOTA: Si carga un certificado e intenta verlo inmediatamente, aparecerá un mensaje de error que indica que la operación solicitada no puede realizarse. Esto sucede porque el servidor web está en el proceso de reinicio con el certificado nuevo. Después de que el servidor web se reinicia, el certificado se carga satisfactoriamente y se puede ver el certificado nuevo. Después de cargar un certificado, es posible que haya una demora de alrededor de un minuto para poder ver el certificado cargado.

NOTA: Puede cargar cada certificado autofirmado (generado mediante la función CSR) solo una vez. Cualquier intento de cargar el certificado por segunda vez no se completará, ya que la clave privada se elimina después de la primera carga del certificado.

Carga del certificado del servidor mediante la interfaz web del CMC

Para cargar un certificado de servidor mediante la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Chassis Overview (Descripción general del chasis)** y luego haga clic en **Network (Red)** > **SSL**. Aparecerá **SSL Main Menu (Menú principal de SSL)**.
2. Seleccione la opción **Cargar certificado de servidor según CSR generada** y haga clic en **Siguiente**.
3. Haga clic en **Elegir archivo** y especifique el archivo del certificado.
4. Haga clic en **Aplicar**. Si el certificado no es válido, se mostrará un mensaje de error.

   NOTA: El valor **File Path (Ruta de acceso del archivo)** muestra la ruta de acceso relativa del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso absoluta del archivo, que incluye la ruta de acceso completa más el nombre completo del archivo con la extensión.

Carga del certificado del servidor mediante RACADM

Para cargar el certificado de servidor SSL, utilice el comando `sslcertupload`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Carga de clave y certificado de Web Server

Puede cargar una clave de servidor web y un certificado de servidor para la clave de servidor web. El certificado de servidor lo expide la autoridad de certificados (CA).

El certificado de servidor web es un componente esencial que se utiliza en el proceso de cifrado SSL. Se autentifica en un cliente compatible con SSL y permite que el cliente se autentifique en el servidor, con lo que ambos sistemas pueden establecer una conexión cifrada.

NOTA: Para cargar una clave de Web Server y un certificado de servidor, es necesario tener privilegios de **Administrador de configuración del chasis**.

Carga de clave y certificado de Web Server mediante la interfaz web del CMC

Para cargar una clave y un certificado de Web Server mediante la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Chassis Overview (Descripción general del chasis)** y haga clic en **Network (Red)** > **SSL**. Aparecerá **SSL Main Menu (Menú principal de SSL)**.
2. Seleccione la opción **Cargar clave y certificado de Web Server** y haga clic en **Siguiente**.
3. Haga clic en **Elegir archivo** para especificar el archivo de clave privada y el archivo de certificado.
4. Una vez cargados los dos archivos, haga clic en **Apply (Aplicar)**. Si el certificado y la clave del servidor web no coinciden, aparecerá un mensaje de error.

   NOTA: La CMC acepta solamente certificados X509 codificados en base 64. No se aceptan los certificados que utilizan otros esquemas de codificación, como DER. La carga de un certificado nuevo reemplaza el certificado predeterminado que recibió con la CMC.

   Una vez que se ha cargado el certificado correctamente, la CMC se restablece y temporalmente deja de estar disponible. Para evitar la desconexión de otros usuarios durante el restablecimiento, notifique a los usuarios autorizados que puedan conectarse a la CMC y busque sesiones activas en la página **Sessions (Sesiones)**, en la ficha **Network (Red)**.

Carga de clave y certificado de Web Server mediante RACADM

Para cargar la clave de SSL desde el cliente en el iDRAC, escriba el siguiente comando:

```
racadm sslkeyupload -t <type> -f <filename>
```

Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Visualización del certificado del servidor

Es posible ver el certificado de servidor SSL que se utiliza actualmente en el CMC.

Visualización del certificado del servidor mediante la interfaz web

En la interfaz web de la CMC, vaya a **Chassis Overview (Descripción general del chasis)** > **Network (Red)** > **SSL**. Seleccione **View Server Certificate (Ver certificado del servidor)** y haga clic en **Next (Siguiente)**. La página **View Server Certificate (Ver certificado del servidor)** muestra el certificado del servidor SSL usado actualmente. Para obtener más información, consulte *CMC Online Help* (Ayuda en línea para la CMC).

NOTA: El certificado del servidor mostrará el nombre común como nombre del bastidor junto al nombre de dominio, si está disponible. En caso contrario, aparecerá solo el nombre del bastidor.

Visualización del certificado del servidor mediante RACADM

Para ver el certificado de servidor SSL, utilice el comando `sslcertview`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

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 a través de RACADM mediante el archivo de configuración

Mediante el archivo de configuración, puede configurar una o varias CMC con propiedades idénticas a través de RACADM.

Cuando busca una tarjeta de CMC específica con las Id. de grupo y de objeto de la tarjeta, RACADM crea el archivo de configuración racadm.cfg a partir de la información obtenida. Al exportar el archivo a una o varias CMC, usted puede configurar sus controladoras con propiedades idénticas de manera muy rápida.

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

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

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

2. Abra una sesión remota de RACADM en el CMC, inicie sesión y escriba:

   ```
   racadm getconfig -f myfile.cfg
   ```

   NOTA: El redireccionamiento de la configuración de la CMC a 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). Cualquier carácter de formato especial en el archivo de configuración puede dañar la base de datos de RACADM.
4. Use el archivo de configuración recién 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` (paso 1) solicita la configuración de la CMC para la CMC activa y genera el archivo `myfile.cfg`. Si es necesario, puede cambiar el nombre del archivo o guardarlo en una ubicación diferente.

   Es posible utilizar el comando getconfig para realizar las siguientes acciones:

- Mostrar todas las propiedades de configuración en un grupo (especificado por el nombre del grupo y el índice)
- Mostrar todas las propiedades de configuración de usuario por nombre de usuario

El subcomando `config` carga la información en otras CMC. El administrador del servidor utiliza el comando `config` para sincronizar la base de datos de usuarios y contraseñas.

Tareas relacionadas

Creación de un archivo de configuración del CMC en la página 99

Creación de un archivo de configuración del CMC

El archivo de configuración de la CMC, `<filename>.cfg`, se utiliza con el comando `racadm config -f <filename>.cfg` para crear un archivo de texto simple. El comando le permite generar un archivo de configuración (similar a un archivo `.ini`) y configurar la CMC desde este archivo.

Se puede utilizar cualquier nombre de archivo y el archivo no requiere una extensión `.cfg` (aunque en este apartado se haga referencia al archivo con esa denominación).

NOTA: Para obtener más información acerca del subcomando `getconfig`, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

RACADM analiza el archivo `.cfg` cuando se carga por primera vez en la CMC, para verificar que haya presentes nombres de objetos y grupos válidos y que se sigan ciertas reglas de sintaxis simples. Los errores se indican con el número de línea que ha detectado el error, y un mensaje explica el problema. Se analiza todo el archivo para verificar su integridad, y se muestran todos los errores. Los comandos de escritura no se transmiten a la CMC si se encuentra un error en el archivo `.cfg`. Usted debe corregir todos los errores antes de poder definir cualquier configuración.

Para verificar si existen errores antes de crear el archivo de configuración, utilice la opción `-c` con el subcomando `config`. Con la opción `-c`, `config` solo verifica la sintaxis y no escribe en la CMC.

Siga estas pautas para crear un archivo `.cfg`:

- Si el analizador encuentra un grupo indexado, el valor del objeto anclado es el que distingue a los diversos índices.

  El analizador lee todos los índices de la CMC de ese grupo. Todos los objetos dentro de ese grupo son modificaciones cuando se configura la CMC. Si un objeto modificado representa un índice nuevo, el índice se crea en la CMC durante la configuración.

- El usuario no puede especificar un índice deseado en un archivo `.cfg`.

  Los índices se pueden crear y se pueden eliminar. Con el tiempo, el grupo se puede fragmentar con índices utilizados y no utilizados. Si hay un índice, se lo modifica. Si no hay un índice, se utiliza el primer índice disponible.

  Este método ofrece flexibilidad al agregar entradas indexadas en las que no es necesario establecer correspondencias exactas entre todas las CMC administradas. Los nuevos usuarios se agregan al primer índice disponible. Un archivo `.cfg` que se analiza y se ejecuta correctamente en una CMC puede no ejecutarse correctamente en otra si todos los índices están llenos y se debe agregar un nuevo usuario.

- Use el subcomando `racresetcfg` para configurar ambas CMC con propiedades idénticas.

  Utilice el subcomando `racresetcfg` para restablecer los valores predeterminados originales de la CMC y, a continuación, ejecute el comando `racadm config -f <filename>.cfg`. Asegúrese de que el archivo `.cfg` incluya todos los objetos, usuarios, índices y demás parámetros que desee. Para ver una lista completa de los objetos y grupos, consulte el capítulo sobre propiedades de la base de datos de *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

  PRECAUCIÓN: Utilice el subcomando `racresetcfg` para restablecer la configuración predeterminada original de la interfaz de red de la CMC, y eliminar todos los usuarios y las configuraciones de usuario. Si bien el usuario raíz está disponible, también se restablecen los valores predeterminados en la configuración de los demás usuarios.

- Si escribe `racadm getconfig -f <filename> .cfg`, el comando crea un archivo `.cfg` para la configuración actual de la CMC. Este archivo de configuración se puede usar como ejemplo y como punto de partida para su archivo `.cfg`.

Conceptos relacionados

Reglas de análisis en la página 100

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 pueden incluir caracteres # en sus cadenas. No se requiere un carácter de escape. Quizás desee generar un `.cfg` desde un comando `racadm getconfig -f <filename> .cfg` y luego ejecutar un comando `racadm config -f <filename> .cfg` para una CMC diferente, sin agregar caracteres de escape.

  Por ejemplo:

  ```
  #
  # This is a comment
  [cfgUserAdmin]
  cfgUserAdminPageModemInitString= <Modem init # not
  a comment>
  ```

- Todas las anotaciones de grupos deben estar entre corchetes de apertura y de cierre ([y]).

  El carácter de apertura [que indica un nombre de grupo debe estar en la columna uno. Este nombre de grupo debe especificarse antes de cualquiera de los objetos de ese grupo. Los objetos que no incluyen un nombre de grupo asociado generarán errores. Los datos de la configuración están organizados en grupos de acuerdo con lo definido en el capítulo sobre propiedades de la base de datos de *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*. 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. No se hace caso a los espacios en blanco que se incluyan después del valor. Los espacios en blanco dentro de las cadenas de valores no se modifican. Los caracteres a la derecha de = (por ejemplo, un segundo =, un #, [,], etc.) se toman tal como figuran. Estos caracteres son caracteres de secuencia de comandos de chat de módem válidos.

  ```
  [cfgLanNetworking] -{group name}
  cfgNicIpAddress=143.154.133.121 {object value}
  ```

- El analizador del archivo `.cfg` ignora una anotación de objeto de índice.

  Usted no puede especificar qué índice se debe utilizar. Si el índice ya existe, se utiliza ese o se crea la nueva entrada en el primer índice disponible para dicho grupo.

  El comando `racadm getconfig -f <filename>.cfg` coloca un comentario antes de los objetos del índice, para que pueda 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 en los archivos `.cfg`. Si elimina la línea con un editor de texto, RACADM se detendrá al analizar el archivo de configuración y generará una alerta de 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 objeto anclado debe ser el primer objeto después del par [ ]. A continuación se proporcionan ejemplos de los grupos indexados actuales:

```
[cfgUserAdmin]
cfgUserAdminUserName= <USER_NAME>
```

- Cuando se utiliza RACADM remoto para capturar los grupos de configuración en un archivo, si no se define una propiedad clave dentro del grupo, el grupo de configuración no se guarda como parte del archivo de configuración. Para replicar estos grupos de configuración en otras CMC, establezca la propiedad clave antes de ejecutar el comando `getconfig -f`. Otra opción es introducir las propiedades que faltan en el archivo de configuración manualmente después de ejecutar el comando `getconfig -f` . Esto se aplica a todos los grupos indexados de racadm.

  Esta es la lista de todos los grupos indexados que exhiben este comportamiento y sus propiedades clave correspondientes:

  - cfgUserAdmin — cfgUserAdminUserName
  - cfgEmailAlert — cfgEmailAlertAddress
  - cfgTraps — cfgTrapsAlertDestIPAddr
  - cfgStandardSchema — cfgSSADRoleGroupName
  - cfgServerInfo — cfgServerBmcMacAddress

Modificación de la dirección IP del CMC

Cuando modifique la dirección IP de la CMC en el archivo de configuración, retire todas las entradas `<variable> = <value>` innecesarias. Solo queda la etiqueta del grupo de variables actual con [and], incluidas las dos entradas `<variable> = <value>` relacionadas con el cambio en la dirección IP.

Por ejemplo:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=192.168.2.110
cfgNicGateway=192.168.2.1
```

Este archivo se actualiza de la siguiente forma:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=192.168.1.143
# comment, the rest of this line is ignored
cfgNicGateway=192.168.1.1
```

El comando `racadm config -f <myfile>.cfg` analiza el archivo e identifica los errores por número de línea. Un archivo correcto actualiza las entradas correctas. Además, puede usar el mismo comando `getconfig` del ejemplo anterior para confirmar la actualización.

Utilice este archivo para descargar cambios que abarcan a 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`.

Visualización y terminación de sesiones en el CMC

Es posible ver el número de usuarios actualmente conectados en iDRAC y terminar las sesiones de usuario.

NOTA: Para terminar una sesión, debe tener privilegios de **Administrador de configuración del chasis**.

Visualización y terminación de sesiones en el CMC mediante la interfaz web

Para ver o terminar una sesión mediante la interfaz web:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Red** > **Sesiones**.

   La página **Sessions (Sesiones)** muestra la Id. de la sesión, el nombre de usuario, la dirección IP y el tipo de sesión. Para obtener más información sobre estas propiedades, consulte *CMC Online Help (Ayuda en línea de la CMC)*.

2. Para finalizar la sesión, haga clic en **Terminar** para una sesión.

Visualización y terminación de sesiones en el CMC mediante RACADM

Es necesario disponer de privilegios de administrador para terminar sesiones en el CMC mediante RACADM.

Para ver las sesiones de usuario actuales, utilice el comando `getssninfo`.

Para terminar la sesión de un usuario, utilice el comando `closessn`.

Para obtener más información acerca de estos comandos, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Configuración de Modo de refrigeración mejorado para ventiladores

La función Modo de refrigeración mejorado (ECM) ofrece refrigeración adicional a través de los ventiladores M1000e de tercera generación. Este modo para ventiladores solo se encuentra disponible cuando las nueve ranuras de ventiladores contienen los nuevos ventiladores M1000e de tercera generación. Los nuevos ventiladores M1000e de tercera generación ofrecen:

- Un nivel de refrigeración superior en los servidores blade comparado con las generaciones anteriores de ventiladores M1000e, cuando la función ECM se encuentra activada.
- El equivalente de refrigeración a las generaciones anteriores de ventiladores M1000e con la misma alimentación, cuando la función ECM se encuentra desactivada.

El modo ECM se recomienda para:

- Las configuraciones de servidores blade con procesadores de potencia de diseño térmico (TDP) alta.
- Las cargas de trabajo donde el rendimiento es fundamental.
- Los sistemas implementados en entornos donde la temperatura de entrada es mayor a 30°C [86°F].

,

NOTA: En ECM, la nueva generación de ventiladores ofrece mayor refrigeración que la generación actual de ventiladores del chasis M1000e. Este aumento en el nivel de refrigeración no siempre es necesario, y se obtiene a expensas de un aumento acústico (el sistema puede generar hasta un 40% más de ruido) y de un mayor consumo de los ventiladores del sistema. La función ECM se puede activar o desactivar según la refrigeración necesaria para el chasis.

La función ECM viene desactivada en el chasis de manera predeterminada. Las acciones de activación y desactivación de ECM quedan marcadas en los registros de la CMC. El estado del modo ECM se conserva incluso después las conmutaciones por fallas de la CMC y los ciclos de encendido de CA del chasis.

Es posible activar o desactivar la función ECM mediante la interfaz web del CMC o la interfaz de línea de comandos (CLI) de RACADM.

Configuración de Modo de refrigeración mejorado para ventiladores mediante la interfaz web

Para configurar la opción Modo de refrigeración mejorado (ECM) en los ventiladores mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Ventiladores** > **Configuración**.
   Se mostrará la página **Configuración avanzada de ventiladores**.

NOTA: Si ECM se encuentra desactivado y ninguno de los ventiladores en el chasis admite la función ECM, no se muestra la ficha **Configuración** para acceder a la página **Configuración avanzada de ventiladores**.

2. En la sección **Configuración de ventiladores**, en el menú desplegable **Modo de refrigeración mejorado**, seleccione **Activar** o **Desactivar**.

   Para obtener más información sobre las descripciones de los campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

   NOTA:

   La opción **Modo de refrigeración mejorado** se puede seleccionar únicamente si:

   - Todos los ventiladores del chasis admiten la función ECM. En este caso, puede activar o desactivar el modo ECM.
   - El modo ECM ya se ha activado y la configuración de ventiladores se ha cambiado a modo mixto, o ningún ventilador admite el modo ECM. En este caso, se puede desactivar el modo ECM, pero no se puede volver a activar hasta que todos los ventiladores del chasis admitan ECM.

   NOTA: Las opciones **Modo de refrigeración mejorado** y **Aplicar** se encuentran atenuadas si:

   - El modo ECM ya se ha desactivado, y la configuración de ventiladores se compone de ventiladores no admitidos y ventiladores admitidos. La sección de información muestra un mensaje con una lista de los ventiladores incompatibles con la función ECM.
   - Ya se ha desactivado el modo ECM y se ha activado la opción **Max Power Conservation Mode (Modo de conservación máx. de alimentación)** (MPCM). La sección de información muestra un mensaje donde se indica que ECM no se admite cuando está activado MPCM.

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

   Si la función ECM se encuentra desactivada, no se puede volver a activar esa función hasta que todos los ventiladores en el chasis admitan ECM.

3. Haga clic en **Aplicar**.
   Cuando la opción ECM se activa o desactiva correctamente, se muestra un mensaje de operación satisfactoria. El modo ECM no se activa si:

   - La alimentación adicional necesaria para los ventiladores admitidos no se encuentra disponible.
   - Cualquiera de los ventiladores en el chasis no admite ECM.
   - MPCM ya se ha activado.

   Se muestra un mensaje de alerta con el motivo por el cual el modo ECM no se puede activar.

   NOTA: Si intenta activar MPCM cuando el modo ECM se encuentra activado, el estado de ECM cambia a activado pero no admitido.

Configuración de Modo de refrigeración mejorado para ventiladores mediante RACADM

Para activar y configurar la función Modo de refrigeración mejorado en los ventiladores, utilice el siguiente objeto de RACADM en el grupo `cfgThermal`:

```
cfgThermalEnhancedCoolingMode
```

Por ejemplo, para activar el modo ECM, utilice:

```
racadm config -g cfgThermal -o cfgThermalEnhancedCoolingMode 1
```

Si surgen errores, aparece un mensaje. El valor predeterminado de la opción Modo de refrigeración mejorado es Desactivado (0). Este valor se configura como Desactivado (0) cuando se emite el comando `racresetcfg`.

Para ver el modo ECM actual, utilice:

```
racadm getconfig -g cfgThermal
```

Para ver el estado actual de ECM, utilice:

```
racadm getfanreqinfo
[Enhanced Cooling Mode]
Enhanced Cooling Mode(ECM) Status  = Disabled
```

Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

7

Configuración del servidor

Es posible realizar las siguientes acciones en el servidor:

- Configuración de nombres de las ranuras
- Establecimiento de la configuración de red del iDRAC
- Configuración de los valores de las etiquetas VLAN para el iDRAC
- Configuración del primer dispositivo de inicio
- Configuración de FlexAddress para el servidor
- Configuración de recurso compartido de archivos remotos
- Configuración de los valores 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 15** caracteres ASCII no extendidos (códigos ASCII 32 a 126). Se permite también el uso de caracteres estándar y especiales en los nombres.
- Los nombres de las ranuras no pueden repetirse dentro de un chasis. No puede haber dos ranuras con el mismo nombre.
- Las cadenas no distinguen entre mayúsculas y minúsculas. `Server-1, server-1, and SERVER-1` son el mismo nombre.
- Los nombres de las ranuras no deben comenzar con las siguientes cadenas:
  - `Switch-`
  - `Fan-`
  - `PS-`
  - `KVM`
  - `DRAC-`
  - `MC-`
  - `Chassis`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- Las cadenas `Server-1` a `Server-16` se pueden utilizar, pero solo para la ranura correspondiente. Por ejemplo, `Server-3` es un nombre válido para la ranura 3, pero no para la ranura 4. Tenga en cuenta que `Server-03` es un nombre válido para cualquier ranura.

  NOTA: Para cambiar un nombre de ranura, es necesario contar con privilegios de **Administrador de configuración del chasis**.

La configuración de nombres de ranuras en la interfaz web reside solo en la CMC. Si un servidor se retira del chasis, la configuración de nombres de ranuras no se conserva con el servidor.

La configuración de nombres de ranuras no se extiende al iKVM opcional. La información de nombres de ranuras está disponible a través de la FRU del iKVM.

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 árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** > **Server Overview (Descripción general del servidor)** y haga clic en **Setup (Configuración)** > **Slot Names (Nombres de las ranuras)**. Aparecerá la página **Slot Names (Nombres de las ranuras)**.
2. En el campo **Slot Name (Nombre de ranura)**, edite el nombre de la ranura. Repita este paso con cada ranura a la que desee cambiarle el nombre.
3. Para utilizar el nombre de host del servidor como nombre de ranura, seleccione la opción **Use Host Name for Slot Name (Utilizar nombre de host para el nombre de ranura)**. Esta opción sustituye los nombres de ranura estáticos con los nombres de host (o los nombres del sistema) del servidor, si se encuentra disponible.

   NOTA: Para utilizar **Use Host Name for Slot Name (Utilizar nombre de host para el nombre de ranura)**, debe instalar el agente de OMSA en el servidor. Para obtener más detalles acerca del agente de OMSA, consulte *Dell OpenManage Server Administrator User's Guide (Guía del usuario de Dell OpenManage Server Administrator)*.

4. Para utilizar el nombre DNS de la iDRAC como nombre de ranura, seleccione la opción **Use iDRAC DNS Name for Slot Name (Utilizar nombre DNS de la iDRAC para el nombre de ranura)**. Esta opción sustituye los nombres de ranura estáticos con los nombres DNS de la iDRAC correspondientes, si se encuentra disponible. Si los nombres DNS de la 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. Haga clic en **Aplicar** para guardar la configuración.
6. Para restaurar el nombre de ranura predeterminado (**RANURA-01** a **RANURA-16**, en función de la ubicación de la ranura del servidor) al servidor, haga clic en **Restaurar valor predeterminado**.

Establecimiento de la configuración de red del iDRAC

Puede determinar la configuración de red de la iDRAC en los servidores instalados o recién insertados. Un usuario puede configurar uno o varios dispositivos iDRAC instalados. También puede ajustar la configuración de red predeterminada de la iDRAC y la contraseña raíz para los servidores que se instalen posteriormente; esta configuración predeterminada es la configuración de QuickDeploy para la iDRAC.

Para obtener más información sobre el iDRAC, consulte *iDRAC User's Guide* (Guía del usuario del iDRAC) en **dell.com/support/manuals**.

Tareas relacionadas

Configuración de los valores de red de QuickDeploy del iDRAC en la página 106
Modificación de la configuración de red del iDRAC en un servidor individual en la página 109
Modificación de la configuración de red del iDRAC mediante RACADM en la página 110

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. Después de activar QuickDeploy, su configuración se aplica a los servidores cuando se instalan.

Para activar y establecer los valores de QuickDeploy del iDRAC mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Server Overview (Descripción general del servidor)** y haga clic en **Setup (Configuración)** > **iDRAC**. Aparecerá la página **Implementar iDRAC**.
2. En la sección **Configuración de QuickDeploy**, especifique la configuración que se muestra en la siguiente tabla.

Tabla 17. : Configuración de QuickDeploy

Configuración	Descripción
QuickDeploy activada	Activa o desactiva la función **QuickDeploy** que aplica automáticamente en los servidores recién insertados la configuración de iDRAC definida en esta página. La configuración automática se debe confirmar de forma local en el panel LCD. **NOTA:** Esto incluye la contraseña de usuario raíz si se selecciona la casilla **Definir contraseña raíz al insertar servidor**.

Tabla 17. : Configuración de QuickDeploy (continuación)

Configuración	Descripción
	De forma predeterminada, esta opción está desactivada.
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 Only (QuickDeploy solamente)**: Seleccione esta opción para aplicar la configuración de red de iDRAC cuando se inserta un servidor nuevo en el chasis. La configuración de implementación automática especificada se usa para configurar el nuevo iDRAC, incluida la contraseña de usuario raíz si se selecciona Cambiar contraseña raíz. ● **Perfil del servidor solamente**: seleccione esta opción para aplicar el perfil del servidor asignado cuando se inserta un servidor nuevo en el chasis ● **QuickDeploy y perfil del servidor**: seleccione esta opción para aplicar primero la configuración de red del iDRAC y, a continuación, el perfil del servidor asignado cuando se inserta un servidor nuevo en el chasis.
Definir contraseña root del iDRAC al insertar servidor	Especifica si una contraseña raíz del iDRAC del servidor debe cambiarse por el valor proporcionado en el campo **Contraseña raíz del iDRAC** al insertar el servidor.
Contraseña root del iDRAC	Cuando se seleccionan las opciones **Set iDRAC Root Password on Server Insertion (Definir contraseña raíz de iDRAC al insertar servidor)** y **QuickDeploy Enabled (QuickDeploy activada)**, este valor de contraseña se asigna a la contraseña de usuario raíz de la iDRAC de los servidores cuando se insertan en el chasis. La contraseña puede tener de 1 a 20 caracteres imprimibles (incluidos los espacios).
Confirmar contraseña root del iDRAC	Verifica la contraseña que se introdujo en el campo **Contraseña raíz del iDRAC**.
Activar LAN del iDRAC	Activa o desactiva el canal LAN de la iDRAC. De forma predeterminada, esta opción está desactivada.
Activar IPv4 del iDRAC	Activa o desactiva IPv4 en la iDRAC. De forma predeterminada, esta opción está activada.
Activar la IPMI en la LAN del iDRAC	Activa o desactiva la IPMI en canal LAN para cada iDRAC presente en el chasis. Está desactivado de manera predeterminada.
Activar DHCP 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. De forma predeterminada, esta opción está desactivada.
Direcciones IP de QuickDeploy reservadas	Le permite seleccionar la cantidad de direcciones IPv4 estáticas reservadas para las 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. La cantidad máxima de direcciones IP estáticas reservadas para: ● los servidores de un cuarto de altura es 32 direcciones IP. ● los servidores de altura media es 16 direcciones IP. ● los servidores de altura total es 8 direcciones IP. **NOTA:** Tenga en cuenta lo siguiente: ● Los valores de cantidad de direcciones IP que son inferiores al valor mínimo requerido para un tipo de servidor se muestran atenuados. ● Si se selecciona una opción inferior al valor predeterminado de cantidad de direcciones IP reservadas, se muestra un mensaje de error donde se advierte que la reducción de la cantidad de direcciones IP evita la implementación rápida de perfiles en los servidores de mayor capacidad. ● Se registra un mensaje de advertencia en el registro de hardware de CMC (SEL) y se genera una alerta SNMP. ● El aviso de implementación rápida no se muestra en el panel LCD si se inserta un servidor de mayor capacidad en una ubicación inferior y la función QuickDeploy se encuentra activada. Para ver la opción de implementación rápida en el panel

Tabla 17. : Configuración de QuickDeploy (continuación)

Configuración	Descripción
	LCD para los servidores de mayor capacidad, regrese las direcciones IP a su valor predeterminado y vuelva a colocar los servidores de mayor capacidad. **NOTA:**
Dirección IPv4 inicial del iDRAC (ranura 1)	Especifica la dirección IP estática del iDRAC del servidor en la ranura 1 del gabinete. La dirección IP de cada iDRAC subsiguiente se incrementa en 1 para cada ranura a partir de la dirección IP estática de la ranura 1. En el caso donde la suma de la dirección IP y del número de ranura sea mayor que la máscara de subred, se mostrará un mensaje de error. **NOTA:** La máscara de subred y la puerta de enlace no se incrementan como la dirección IP. Por ejemplo, si la dirección IP inicial es `192.168.0.250` y la máscara de subred es `255.255.0.0`, la dirección IP de QuickDeploy para la ranura 15 es `192.168.0.265`. Cuando usted intenta definir los valores de los campos de dirección IP inicial, direcciones IP reservadas y máscara de subred de un modo que la combinación pueda generar una dirección IP fuera de la subred, el mensaje de error `QuickDeploy IP address range is not fully within QuickDeploy Subnet` aparece al hacer clic en **Save QuickDeploy Settings (Guardar configuración de QuickDeploy)** o **Auto-Populate Using QuickDeploy Settings (Completar automáticamente con la configuración de QuickDeploy)**. Por ejemplo, si la IP inicial es `192.168.1.245`, la cantidad de direcciones IP reservadas es 16 y la máscara de subred es `255.255.255.0`, las direcciones IP que se generan para las ranuras superiores a la 11 quedan fuera de la subred. Por ende, al intentar definir esta combinación para la configuración de QuickDeploy genera un mensaje de error.
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 iDRAC 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 activada.
Puerta de enlace IPv6 del iDRAC	Especifica la puerta de enlace predeterminada IPv6 para asignarla a los iDRAC. El valor predeterminado es "::".
Longitud del prefijo IPv6 del iDRAC	Especifica la longitud del prefijo para asignar a las direcciones IPv6 del iDRAC. El valor predeterminado es 64.
Utilice los valores de DNS de la CMC	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.

3. Haga clic en **Guardar configuración de QuickDeploy** para guardar la configuración. Si ha realizado cambios en la configuración de red del iDRAC, haga clic en **Aplicar configuración de red del iDRAC** para implementar la configuración en el iDRAC.

   La función QuickDeploy solamente se ejecuta cuando está activada y se inserta un servidor en el chasis. Si las opciones **Set iDRAC Root Password on Server Insertion (Definir contraseña raíz de iDRAC al insertar servidor)** y **QuickDeploy Enabled (QuickDeploy activada)** están activadas, se preguntará al usuario de la interfaz LCD si permite o impide el cambio de la contraseña. Si existen valores de configuración de red que difieren de la configuración actual de la iDRAC, se le pide al usuario que acepte o rechace los cambios.

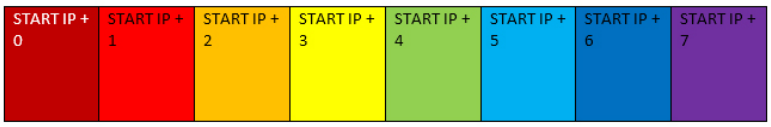
   NOTA: Cuando existe una diferencia en la LAN o en la IPMI en canal LAN, se le solicita al usuario que acepte el valor de dirección IP de QuickDeploy. Si la diferencia es la configuración de DHCP, se le pide al usuario que acepte el valor de QuickDeploy para DHCP.

   Para copiar la configuración de QuickDeploy a la sección **Configuración de red del iDRAC**, haga clic en **Completar automáticamente con la configuración de QuickDeploy**. Los valores de configuración de red de QuickDeploy se copian en los campos correspondientes de la tabla **Valores de configuración de red del iDRAC**.

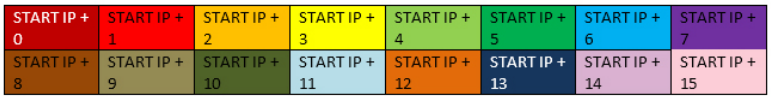
NOTA: Los cambios realizados en los campos de QuickDeploy son inmediatos, pero es posible que se necesiten unos minutos para que los cambios realizados en uno o más valores de configuración de red de servidores de la iDRAC se propaguen de la CMC a la iDRAC. Al hacer clic en **Refresh (Actualizar)** demasiado rápido, es posible que solo se muestren datos parcialmente correctos de uno o varios servidores iDRAC.

Asignación de direcciones IP de QuickDeploy para servidores

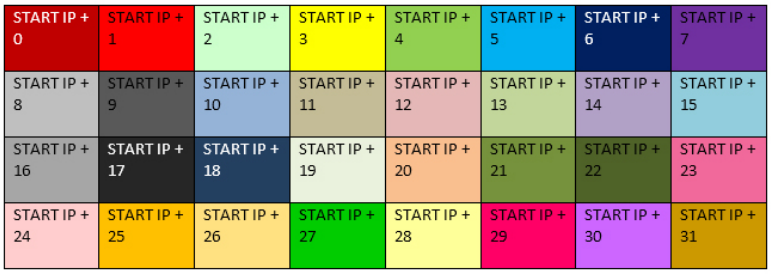
En la figura se muestra la asignación de direcciones IP de QuickDeploy a los servidores cuando hay ocho servidores de altura completa en un chasis M1000e:



En la figura siguiente se muestra la asignación de direcciones IP de QuickDeploy a los servidores cuando hay 16 servidores de altura media en un chasis M1000e:



En la figura siguiente se muestra la asignación de direcciones IP de QuickDeploy a los servidores cuando hay 32 servidores de un cuarto de altura en un chasis M1000e:



Configuración de direcciones IP de QuickDeploy reservadas mediante RACADM

Para modificar la cantidad de direcciones IP estáticas asignadas a los servidores en el chasis mediante el RACADM, utilice el siguiente comando:

```
racadm deploy -q -n <num>
```

donde <num> es la cantidad de direcciones IP: 8, 16 o 32.

Para ver los valores actuales para la cantidad de direcciones IP reservadas y **Utilizar configuración CMC DNS** para servidores en el chasis mediante RACADM, utilice el siguiente comando:

```
racadm deploy -q
```

Para modificar la opción **Utilizar los valores DNS de CMC** para activar la implementación rápida para los servidores en el chasis mediante RACADM, utilice el siguiente comando:

```
racadm deploy -q -e <enable/disable>
```

Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

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

Con esta tabla, puede definir los valores de configuración de red de la iDRAC para cada servidor instalado. Los valores iniciales que se muestran para cada campo son los valores actuales leídos de la iDRAC.

Para modificar la configuración de red del iDRAC mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Server Overview (Descripción general del servidor)** y haga clic en **Setup (Configuración)** > **iDRAC**. Aparecerá la página **Deploy iDRAC (Implementar iDRAC)**. En la sección **iDRAC Network Settings (Configuración de red de la iDRAC)** se presentan los valores de configuración de las redes IPv4 e IPv6 de iDRAC de todos los servidores instalados.
2. Modifique la configuración de red del iDRAC según sea necesario para los servidores.

   NOTA: Debe seleccionar la opción **Enable LAN (Activar LAN)** para especificar la configuración de IPv4 o IPv6. Para obtener información sobre los campos, consulte CMC Online Help (Ayuda en línea para el CMC).

3. Para implementar la configuración en la iDRAC, haga clic en **Apply iDRAC Network Settings (Aplicar configuración de red de la iDRAC)**. Si realizó cambios en la configuración de QuickDeploy, también se guardan.

   En la tabla **iDRAC Network Settings (Configuración de red de la iDRAC)** se reflejan los valores futuros de la configuración de red; los valores mostrados para los servidores instalados pueden ser o no los mismos que los instalados actualmente. Haga clic en **Refresh (Actualizar)** para actualizar la página **iDRAC Deploy (Implementación de la iDRAC)** con cada valor de configuración de red de la iDRAC instalado después de realizar los cambios.

   NOTA: Los cambios realizados en los campos de QuickDeploy son inmediatos, pero es posible que se necesiten unos minutos para que los cambios realizados en uno o más valores de configuración de red de servidores de la iDRAC se propaguen de la CMC a la iDRAC. Al hacer clic en **Refresh (Actualizar)** demasiado rápido, es posible que solo se muestren datos parcialmente correctos de uno o varios servidores de la iDRAC.

Modificación de la configuración de red del iDRAC mediante RACADM

Los comandos RACADM `config` o `getconfig` admiten la opción `-m <module>` para los grupos de configuración siguientes:

- `cfgLanNetworking`
- `cfgIPv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

Para obtener más información sobre los valores y rangos predeterminados de las propiedades, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

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. Se conservan en el chasis aunque se elimine un componente.

NOTA: La Id. de VLAN configurada mediante la CMC se aplica a la iDRAC solo cuando la iDRAC se encuentra en modo exclusivo. Si la iDRAC está en modo de LOM compartida, los cambios de Id. de VLAN realizados en la iDRAC no se muestran en la GUI de la CMC.

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

Para configurar la red VLAN en el servidor mediante la interfaz web del CMC:

1. Desplácese a cualquiera de las siguientes páginas:
   - En el árbol del sistema, diríjase a **Descripción general del chasis** y haga clic en **Red** > **VLAN** .
   - En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** > **Server Overview (Descripción general del servidor)** y haga clic en **Network (Red)** > **VLAN**. Aparecerá la página **Configuración de la etiqueta VLAN**.
2. En la sección **iDRAC**, active la VLAN para los servidores, establezca la prioridad e introduzca la Id. Para obtener más información acerca de los campos, consulte *CMC Online Help (Ayuda en línea de la CMC)*.

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 1-16.

  Los valores válidos para `<VLAN>` son 1-4000 y 4021-4094. El valor predeterminado es 1.

  Los valores válidos para `<VLAN priority>` son 0-7. 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 1-16.

  Por ejemplo:

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

Configuración del primer dispositivo de inicio

Usted puede especificar el primer dispositivo de inicio de la CMC para cada servidor. Quizás este no sea el primer dispositivo de inicio real para el servidor ni represente un dispositivo presente en ese servidor, sino que representa un dispositivo que la CMC envía al servidor y se utiliza como primer dispositivo de inicio allí.

Es posible establecer el dispositivo de inicio predeterminado y definir un dispositivo de inicio para una sola vez a fin de poder iniciar una imagen que realice tareas como ejecutar diagnósticos o reinstalar un sistema operativo.

Puede configurar el primer dispositivo de inicio para solo el siguiente inicio o para todos los reinicios subsiguientes. Según esta selección, puede definir el primer dispositivo de inicio para el servidor. El sistema se inicia desde el dispositivo seleccionado en los próximos inicios y permanece como 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 del CMC suprime la configuración de inicio del BIOS del sistema.

El dispositivo de inicio que especifique debe existir y contener soportes iniciables.

Es posible establecer los siguientes dispositivos para el primer inicio.

Tabla 18. : Dispositivos de inicio

Dispositivo de inicio	Descripción
PXE	Inicio a partir de un protocolo de entorno de ejecución previa al inicio (PXE) en la tarjeta de interfaz de red.
Unidad de disco duro	Inicio a partir del disco duro del servidor.

Tabla 18. : Dispositivos de inicio (continuación)

Dispositivo de inicio	Descripción
CD/DVD local	Inicio a partir de una unidad de CD/DVD en el servidor.
Disco flexible virtual	Inicio desde la unidad de disco flexible virtual. La unidad de disco flexible (o una imagen del disco flexible) se encuentra en otro equipo de la red de administración y se conecta a través del visor de consola de la GUI de la iDRAC.
CD/DVD virtual	Inicio desde una unidad de CD/DVD virtual o de una imagen ISO de CD/DVD. La unidad óptica o el archivo de imagen ISO se encuentra en otro equipo o disco disponible en la red de administración y se conecta a través del visor de consola de la GUI de la iDRAC.
iSCSI	Inicio a partir de un dispositivo de interfaz estándar de equipos pequeños (iSCSI) de Internet. **NOTA:** Esta opción solo se admite hasta los servidores Dell PowerEdge de 11ª generación.
Tarjeta SD local	Inicio a partir de la tarjeta SD (Secure Digital) local, solo para servidores que admiten el sistema iDRAC.
Disco flexible	Inicio a partir de un disco flexible en la unidad de disco flexible local.
RFS	Inicio desde una imagen de recurso compartido de archivos remotos (RFS). El archivo de imagen se conecta mediante el visor de consola de la GUI de la iDRAC.
Ruta de acceso dispositivo UEFI	Inicio desde la ruta de acceso a dispositivo de la interfaz de firmware extensible unificada (UEFI) del servidor.

Tareas relacionadas

Configuración del primer dispositivo de inicio para varios servidores mediante la interfaz web del CMC en la página 112
Configuración del primer dispositivo de inicio para un servidor individual mediante la interfaz web del CMC en la página 112
Configuración del primer dispositivo de inicio mediante RACADM en la página 113

Configuración del primer dispositivo de inicio para varios servidores mediante la interfaz web del CMC

NOTA: Para configurar el primer dispositivo de inicio para los servidores, es necesario contar con privilegios de **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 mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Server Overview (Descripción general del servidor)** y haga clic en **Setup (Configuración)** > **First Boot Device (Primer dispositivo de inicio)**. Aparecerá una lista de servidores.
2. En el menú desplegable de la columna **Primer dispositivo de inicio**, 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, desmarque la opción **Boot Once (Iniciar una vez)** para el servidor. Si desea que el servidor utilice el dispositivo seleccionado solo en el siguiente ciclo de inicio, seleccione la opción **Boot Once (Iniciar una vez)** para el servidor.
4. Haga clic en **Aplicar** para guardar la configuración.

Configuración del primer dispositivo de inicio para un servidor individual mediante la interfaz web del CMC

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 un servidor individual mediante la interfaz web del CMC:

1. En el sistema, vaya a **Descripción general del servidor** y haga clic en el servidor para el cual desea configurar el primer dispositivo de inicio.
2. Vaya a **Setup (Configuración)** > **First Boot Device (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, desmarque la opción **Boot Once (Iniciar una vez)** para el servidor. Si desea que el servidor utilice el dispositivo seleccionado solo en el siguiente ciclo de inicio, seleccione la opción **Boot Once (Iniciar una vez)** para el 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 una única vez para un dispositivo, utilice el objeto `cfgServerBootOnce` .

Para obtener más información acerca de estos objetos, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Configuración de FlexAddress para el servidor

Para obtener más información sobre la configuración de FlexAddress para el servidor, consulte Configuring FlexAddress for Server-Level Slots (Configuración de FlexAddress para ranuras en el nivel del servidor).

Configuración de recurso compartido de archivos remotos

La función **Recurso compartido de archivos de soporte virtual remoto** asigna un archivo de una unidad compartida en la red a uno o varios servidores a través de la CMC, para implementar o actualizar un sistema operativo. Cuando el archivo remoto se encuentra conectado, se puede acceder a él como si estuviera en el sistema 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 configurar el recurso compartido de archivos remotos mediante la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Descripción general del servidor** y haga clic en **Configuración** > **Recurso compartido de archivos remotos**.
   Aparecerá la página **Implementar recurso compartido de archivos remotos**.
   NOTA: Si alguno de los servidores presentes en las ranuras es de generación 12 o posterior y no tiene la licencia correspondiente, aparece un mensaje para indicar que falta o está vencida una licencia necesaria. Deberá obtener la licencia correspondiente e intentar nuevamente, o bien comunicarse con su proveedor de servicio para conocer más detalles.
2. Especifique la configuración necesaria. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
3. Haga clic en **Connect (Conectar)** para conectarse a un recurso compartido de archivos remoto. Para conectarse a un recurso compartido de archivos remoto, debe proporcionar la ruta de acceso, 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: Guarde todos los archivos de trabajo antes de seleccionar la opción **Implementar** para implementar el dispositivo de medios, ya que esta acción provoca el reinicio del servidor.

   Esta acción implica lo siguiente:
   - El recurso compartido de archivos remotos se conecta.

- El archivo se selecciona como primer dispositivo de inicio de los servidores.
- El servidor se reinicia.
- Si el servidor está apagado se enciende.

Configuración de las opciones de perfil con la replicación de configuración de servidores

La función de replicación de configuración de servidores le permite aplicar, en uno o más servidores, todas las opciones de perfil de un servidor especificado. Las opciones de perfil que pueden replicarse son las que pueden modificarse y están pensadas para replicarse en servidores. Se muestran y se pueden replicar los siguientes tres grupos de perfiles de servidores:

- BIOS: este grupo incluye solo los valores del BIOS de un servidor. Estos perfiles se generan desde las versiones de CMC anteriores a 4.3.
- BIOS e inicio: este grupo incluye los valores del BIOS y de inicio de un servidor. Estos perfiles se generan desde:
  - CMC versión 4.3
  - CMC versión 4.45 con servidores de 11.ª generación
  - CMC versión 4.45 y servidores de 12.ª generación con Lifecycle Controller 2 de una versión anterior a la 1.1
- Todas las opciones: Esta versión incluye todas las opciones de configuración del servidor y los componentes de ese servidor. Estos perfiles se generan desde:
  - CMC versión 4.45 y servidores de 12.ª generación con iDRAC y Lifecycle Controller 2 versión 1.1 o posterior.
  - CMC versión 5.0 y servidores de 13.ª generación con iDRAC con Lifecycle Controller 2.00.00.00 o posterior

La función de replicación de configuración de servidores admite servidores iDRAC y posteriores. Los servidores RAC de generaciones anteriores se muestran en la lista pero aparecen atenuados en la página principal, porque no pueden usar esta función.

Para usar la función de replicación de configuración de servidores:

- Debe tener la versión mínima requerida del iDRAC. Los servidores iDRAC requieren, como mínimo, la versión 3.2 y 1.00.00.
- El servidor debe estar encendido.

Versiones de servidores y compatibilidades de perfiles:

- iDRAC con Lifecycle Controller 2 versión 1.1 y posterior puede aceptar cualquier versión de perfil.
- iDRAC versión 3.2 e 1.0 solo acepta perfiles de BIOS o de BIOS e inicio.
- Si guarda un perfil de un servidor iDRAC con Lifecycle Controller 2 versión 1.1 y posteriores, se crea un perfil de Todas las opciones. Al guardar un perfil de un servidor con iDRAC versión 3.2 e iDRAC con Lifecycle Controller 2 versión 1.0, se crea un perfil de BIOS e inicio.

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.

Tareas relacionadas

Acceso a la página Perfiles de servidores en la página 114
Agregar o guardar perfil en la página 115
Aplicación de un perfil en la página 115
Visualizar configuración de perfil en la página 117
Visualización del registro de perfiles en la página 118
Estado de finalización, vista de registros, y solución de problemas en la página 118

Acceso a la página Perfiles de servidores

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

Para acceder a la página **Server Profiles (Perfiles de servidor)** con la interfaz web de la CMC, en el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** > **Server Overview (Descripción general del servidor)**. Haga clic en **Setup (Configuración)** > **Profiles (Perfiles)**. Aparecerá la página **Server Profiles (Perfiles de servidor)**.

Tareas relacionadas

Agregar o guardar perfil en la página 115
Aplicación de un perfil en la página 115
Visualizar configuración de perfil en la página 117
Visualización del registro de perfiles en la página 118
Estado de finalización, vista de registros, y solución de problemas en la página 118

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 el soporte de almacenamiento extendido no volátil de la CMC.

NOTA: Si hay 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 del CMC.

La eliminación o desactivación de los medios de almacenamiento extendido no volátiles impide el acceso al perfil almacenado y desactiva la función Configuración de servidores.

Para agregar o guardar un perfil:

1. Diríjase a la página **Server Profiles (Perfiles de servidor)**. En la sección **Server Profiles (Perfiles de servidor)**, seleccione el servidor a partir de cuya configuración desee generar el perfil y, a continuación, haga clic en **Save Profile (Guardar perfil)**. Aparece la sección **Guardar perfil**.
2. Seleccione **Almacenamiento extendido** o **Recurso compartido de red** como la ubicación en la que desea guardar el perfil.

   NOTA: La opción **Recurso compartido de red** está activada y los detalles aparecerán en la sección **Perfiles almacenados** solo si el recurso compartido de red está montado y se puede acceder al mismo. Si el **Network Share (Recurso compartido de red)** no está conectado, configure el recurso compartido de red para el 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** y **Descripción** ingrese el nombre de perfil y la descripción (opcional) y haga clic en **Guardar perfil**.

   NOTA: Al guardar un perfil de servidor, se admite el conjunto de caracteres extendidos ASCII estándar. No obstante, no se admiten los siguientes caracteres especiales:

   ), “, ., *, >, <, \, /, :, |, #, ?, y ,

   El CMC se comunica con Lifecycle Controller 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.

Tareas relacionadas

Acceso a la página Perfiles de servidores en la página 114

Aplicación de un perfil

La clonación de servidores solo es posible cuando hay perfiles de servidor disponibles como perfiles almacenados en los soportes no volátiles de la CMC o en el recurso compartido remoto. Para iniciar una operación de configuración de servidores, puede aplicar un perfil almacenado a uno o más servidores.

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 **Save and Apply Profiles (Guardar y aplicar perfiles)**, seleccione los servidores donde desee aplicar el perfil seleccionado.
   Se activará el menú desplegable **Seleccionar perfil**.
   NOTA: El menú desplegable **Seleccionar perfil** muestra todos los perfiles disponibles clasificados por tipo, incluidos aquellos que se encuentran en el recurso compartido remoto y en 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**.
   Aparecerá un mensaje para advertir 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 replicación de configuraciones de servidores, la opción CSIOR debe estar activada para los servidores. Si esta opción está desactivada, aparecerá un mensaje para advertirlo. Para completar la operación de replicación de configuración de servidor, 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 aplicará a los servidores, los cuales quizás se reinicien de inmediato, de ser necesario. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Tareas relacionadas

Acceso a la página Perfiles de servidores en la página 114

Importar archivo

Puede importar a la CMC un perfil de servidor almacenado en una estación de administración.

Para importar al CMC un perfil almacenado en un recurso compartido de archivos remotos:

1. En la página **Perfiles de servidor**, en la sección **Perfiles almacenados**, haga clic en **Importar perfil**.
   Aparecerá la sección **Importar perfil de servidor**.
2. Haga clic en **Explorar** para acceder al perfil desde la ubicación requerida y luego haga clic en **Importar perfil**.
   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Exportar archivo

Puede exportar un perfil del servidor almacenado que está guardado en los medios no volátiles (tarjeta SD) del CMC a una ruta de acceso específica 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 para indicar que, si exporta el perfil, se perderá la descripción. Presione **OK (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 de 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 modos de exportación alternativos para configuraciones RAID y atributos de identidad, consulte el documento técnico *Server Cloning with Server Configuration Profiles (Clonación de servidores con perfiles de configuración de servidor)*, disponible en **delltechcenter.com**.

Editar perfil

Puede editar el nombre y la descripción de un perfil de servidor que está almacenado en los medios no volátiles del CMC (tarjeta de SD) o el nombre de un perfil de servidor almacenado en el recurso compartido remoto.

Para editar un perfil almacenado:

1. Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Editar perfil**.
   Aparecerá la sección **Editar perfil del servidor— <Nombre de perfil>**.
2. Edite el nombre y la descripción del perfil del servidor según sea necesario y luego haga clic en **Guardar perfil**.
   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Eliminar perfil

Puede eliminar un perfil del servidor que está almacenado en los medios no volátiles del CMC (tarjeta de SD) o en el recurso compartido de red.

Para eliminar un perfil almacenado:

1. En la página **Perfiles del servidor**, en la sección **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Eliminar perfil**.
   Aparecerá un mensaje de advertencia donde se indica que al eliminar un perfil se eliminará permanentemente el perfil seleccionado.
2. Haga clic en **Aceptar** para eliminar el perfil seleccionado.
   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualizar configuración de perfil

Para ver **Profile settings (Configuración de perfil)** en un servidor seleccionado, diríjase a la página **Server Profiles (Perfiles de servidor)**. En la sección **Server Profiles (Perfiles de servidor)**, haga clic en **View (Ver)** en la columna **Server Profile (Perfil de servidor)** del servidor que desee. Aparece la página **Ver configuración**.

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

NOTA: La aplicación Clonación de servidores del CMC recupera y muestra los valores de un servidor específico solamente si la opción **Recolectar inventario del sistema en el reinicio** (CSIOR) se encuentra activada.

Para activar CSIOR en:

- Servidores de 11ª generación: después de reiniciar el servidor, en los valores de **Ctrl-E**, seleccione **Servicios del sistema**, active **CSIOR** y guarde los cambios.
- Servidores de 12ª generación: después de reiniciar el servidor, en los valores de **F2**, seleccione **Configuración del iDRAC** > **Lifecycle Controller**, active **CSIOR** y guarde los cambios.
- Servidores de 13ª generación: Después de reiniciar el servidor, cuando se le solicite, presione **F10** para acceder a Lifecycle Controller. Para ir a la página **Hardware Inventory (Inventario de hardware)**, seleccione **Hardware Configuration (Configuración de hardware)** > **Hardware Inventory (Inventario de hardware)**. En la página **Inventario de hardware** , haga clic en **Recopilar inventario del sistema al reinicio**.

Tareas relacionadas

Acceso a la página Perfiles de servidores en la página 114

Visualización de la configuración de los perfiles almacenados

Para ver la configuración de los perfiles de servidores almacenados en los soportes no volátiles de la CMC (tarjeta SD) o en un recurso compartido de red, vaya a la página **Server Profiles (Perfiles de servidor)**. En la sección **Stored Profiles (Perfiles almacenados)**, haga clic en **View (Ver)** en la columna **View Profile (Ver perfil)** del perfil que desee. Aparece la página **Ver configuración**. Para obtener más información sobre la configuración visualizada, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización del registro de perfiles

Para ver el registro de perfiles, en la página **Perfiles del servidor**, consulte la sección **Registro de perfiles reciente**. En esta sección se presentan las 10 entradas más recientes del registro de perfiles directamente desde las operaciones de configuración de servidores. Cada entrada del registro muestra la gravedad, la fecha y la hora de envío de la operación de configuración de servidores, y la descripción del mensaje del registro de configuración. 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 *CMC Online Help (Ayuda en línea para el CMC)*.

NOTA: Para obtener más información acerca del funcionamiento y del registro asociado en los servidores Dell PowerEdge M4110, consulte la documentación de EqualLogic.

Estado de finalización, vista de registros, y solución de problemas

Para revisar el estado de compleción de un perfil de servidor aplicado:

1. En la página **Perfiles del servidor**, anote el valor de Identificación de trabajo (JID) para el trabajo enviado de la sección **Registro de perfiles reciente**.
2. En el árbol del sistema, vaya a **Server Overview (Descripción general del servidor)** y haga clic en **Troubleshooting (Solución de problemas)** > **Lifecycle Controller Jobs (Trabajos de Lifecycle Controller)**. Busque la misma JID en la tabla **Jobs (Trabajos)**.
3. 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 de servidor. Cualquier servidor que admita la clonación de servidores insertado en dicha ranura se configura mediante el perfil asignado. Puede realizar la acción de implementación rápida solamente si la opción **Action When Server is Inserted (Acción cuando el servidor está insertado)** de la página **Deploy iDRAC (Implementar iDRAC)** está configurada como **Server Profile (Perfil de servidor)** o **Quick Deploy and Server Profile (Implementación rápida y perfil de servidor)**. Si se selecciona una de estas opciones, se permite aplicar el perfil de servidor asignado cuando se inserta un nuevo servidor en el chasis. Para ir a la página **Deploy iDRAC (Implementar iDRAC)**, seleccione **Server Overview (Descripción general del servidor)** > **Setup (Configuración)** > **iDRAC**. Los perfiles que se pueden implementar se encuentran en la tarjeta SD o en el recurso compartido de red. Para configurar los perfiles para implementación rápida, debe tener privilegios de **Administrador del chasis**.

NOTA:

Asignación de perfiles del servidor a ranuras

La página **Server Profiles (Perfiles de servidor)** le permite asignar perfiles de servidor a las 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 de implementación rápida solamente si la opción **Action When Server is Inserted (Acción cuando el servidor está insertado)** de la página Deploy iDRAC (Implementar iDRAC) está configurada como **Server Profile**

(Perfil de servidor) o **Quick Deploy and Server Profile (Implementación rápida y perfil de servidor)**. Si se selecciona una de estas opciones, se permite aplicar el perfil de servidor asignado cuando se inserta un nuevo servidor en el chasis.

2. En el menú desplegable, seleccione el perfil que desea asignar a la ranura requerida. Puede seleccionar un perfil para aplicar a varias ranuras.
3. Haga clic en **Asignar perfil**.
   El perfil se asigna a las ranuras seleccionadas

NOTA:

- Una ranura que no tiene ningún perfil asignado se indica mediante el término "Sin perfil seleccionado" que aparece en el cuadro de selección.
- Para eliminar la asignación de un perfil de una o más ranuras, seleccione las ranuras y haga clic en **Remove Assignment (Quitar asignación)**. Aparecerá un mensaje para advertir que, al quitar un perfil de las ranuras, se elimina la configuración del perfil de todos los servidores insertados en las ranuras si está activada la función **Quick Deploy Profiles (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 **Implementación rápida de perfiles**, el progreso y los resultados de la aplicación se conservan en el registro de perfiles.

NOTA:

- Si no se puede acceder al perfil asignado en el recurso compartido de red cuando se inserta un servidor en la ranura, la pantalla LCD muestra un mensaje que indica que el perfil asignado no está disponible para la ranura <X>.
- La opción **Recurso compartido de red** está activada y los detalles aparecerán en la sección **Perfiles almacenados** solo si el recurso compartido de red está montado y se puede acceder al mismo. Si el recurso compartido de red no está conectado, configure el recurso compartido de red del chasis. Para configurar el recurso compartido de red, haga clic en **Editar** en la sección **Perfiles almacenados**. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web del 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*.

Admin del grupo de direcciones MAC virtuales

Puede crear, agregar, quitar y desactivar direcciones MAC mediante la **Administracion del grupo de direcciones MAC virtuales**. Solo puede usar direcciones MAC de unidifusión en el grupo de direcciones MAC virtuales. Se permiten los siguientes rangos de direcciones MAC en el CMC.

- 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 dirección MAC virtual** mediante la interfaz web del CMC, en el árbol del sistema, vaya a **Visión general del chasis** > **Visión general del servidor**. Haga clic en **Configuración** > **Perfiles** > **Perfiles de identidad de inicio**. Se muestra la sección **Administrar grupo 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 elimina del recurso compartido de red para serializar las operaciones de identidad de inicio desde 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 *Ayuda en línea para el CMC*.

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 administración limitada de los componentes individuales del chasis, como los servidores. Para administrar de forma completa estos componentes individuales, la CMC proporciona un punto de inicio para la interfaz web de la controladora de administración del servidor (iDRAC).

Un usuario puede iniciar la interfaz web de la iDRAC sin necesidad de iniciar sesión por segunda vez, ya que esta función utiliza el inicio de sesión único. Las políticas del inicio de sesión único son las siguientes:

- Un usuario de la CMC con el privilegio de administración de servidores se conecta automáticamente a iDRAC mediante el inicio de sesión único. Una vez en el sitio de la iDRAC, se le otorgan privilegios de administrador automáticamente. Esto sucede incluso cuando el usuario no dispone de cuenta en la iDRAC o la cuenta no tiene privilegios de administrador.
- Un usuario de la CMC **SIN** privilegio de administrador de servidores, pero con la misma cuenta en la iDRAC, se conecta automáticamente a la iDRAC mediante el inicio de sesión único. Una vez en el sitio de la iDRAC, se le otorgan los privilegios creados para la cuenta de la iDRAC.
- Un usuario de la CMC sin privilegio de administrador de servidores ni la misma cuenta en la iDRAC no se conecta automáticamente a la iDRAC mediante el inicio de sesión único. A este usuario se lo dirige a la página de inicio de sesión de la iDRAC cuando hace clic en **Launch iDRAC GUI (Iniciar GUI de iDRAC)**.

NOTA: En este contexto, al decir "la misma cuenta" hablamos de que el usuario tiene el mismo nombre de inicio de sesión y la misma contraseña para la CMC y para la iDRAC. Cuando el usuario tenga el mismo nombre de inicio de sesión pero la contraseña no coincida, no se considerará que 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 **Launch iDRAC GUI (Iniciar GUI de iDRAC)**, puede aparecer una página de error cuando sucede lo siguiente:

- Se retira el servidor del chasis
- Se cambia la dirección IP de la iDRAC
- La conexión de red de la iDRAC tiene algún problema

En MCM, al abrir la interfaz web de la iDRAC desde un chasis miembro, las credenciales del usuario del chasis principal y del chasis miembro deben ser las mismas. De lo contrario, la sesión actual del chasis miembro se anula, y aparece la página de inicio de sesión del chasis miembro.

Tareas relacionadas

Inicio del iDRAC desde la página Estado de los servidores en la página 124
Inicio del iDRAC desde la página Estado del servidor en la página 124

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 árbol del sistema, haga clic en **Server Overview (Descripción general del servidor)**. Aparecerá la página **Estado de los servidores**.
2. Haga clic en **Iniciar iDRAC** para el servidor donde desea que se inicie la interfaz web del iDRAC.

   NOTA: El inicio de la iDRAC puede configurarse a través de la dirección IP o el nombre DNS. El método predeterminado es a través de la dirección IP.

Inicio del iDRAC desde la página Estado del servidor

Para iniciar la consola de administración del iDRAC de un servidor individual:

1. En el árbol del sistema, expanda la opción **Descripción general del servidor**. Todos los servidores (1-16) aparecerán en la lista expandida **Servers (Servidores)**.
2. Haga clic en el servidor para el cual desea iniciar la interfaz web del iDRAC. Se muestra la página **Estado del servidor**.
3. Haga clic en **Launch iDRAC GUI (Iniciar GUI de iDRAC)**. Aparecerá la interfaz web de la iDRAC.

Inicio de la consola remota desde la interfaz web del CMC

Puede iniciar una sesión de KVM (teclado, video y mouse) directamente en el servidor. La función de consola remota solo se admite cuando se cumplen todas las siguientes condiciones:

- El chasis está encendido.
- Servidores que admiten iDRAC.
- La interfaz de LAN en el servidor está activada.
- La versión del iDRAC es 2.20 o superior.
- El sistema host está instalado con JRE (Java Runtime Environment) 6 Update 16 o superior.
- El explorador del sistema host admite el uso de ventanas emergentes (el bloqueo de ventanas emergentes está desactivado).

La consola remota también se puede iniciar desde la interfaz web de la iDRAC. Para conocer más detalles, consulte *iDRAC User's Guide (Guía del usuario de iDRAC)*.

Tareas relacionadas

Inicio de la consola remota desde la página Condición del chasis en la página 124
Inicio de la consola remota desde la página Estado del servidor en la página 125
Inicio de la consola remota desde la página Estado de los servidores en la página 125

Inicio de la consola remota desde la página Condición del chasis

Para iniciar una consola remota desde la interfaz web del CMC, realice alguno de los siguientes pasos:

1. En el árbol del sistema, diríjase a **Chassis Overview (Descripción general del chasis)** y luego haga clic en **Properties (Propiedades)** > **Health (Condición)**. Aparecerá la página **Estado del chasis**.
2. Haga clic en el servidor específico en el gráfico del chasis.
3. En la sección **Vínculos rápidos**, haga clic en el vínculo **Iniciar consola remota** para iniciar la consola remota.

Inicio de la consola remota desde la página Estado del servidor

Para iniciar la consola remota de un servidor individual:

1. En el árbol del sistema, expanda la opción **Descripción general del servidor**.
   Todos los servidores (1 a 16) aparecen en la lista expandida de servidores.
2. Haga clic en el servidor donde desea ejecutar la consola remota.
   Se muestra la página **Estado del servidor**.
3. Haga clic en **Iniciar la consola remota**.

Inicio de la consola remota desde la página Estado de los servidores

Para iniciar la consola remota desde la página **Estado de los servidores**:

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Propiedades** > **Estado**.
   Aparecerá la página **Estado de los servidores**.
2. Haga clic en **Iniciar la consola remota** para el servidor necesario.

8

Configuración del CMC para enviar alertas

Puede configurar alertas y acciones para ciertos sucesos que se producen en el sistema administrado. Un suceso se produce cuando el estado de un componente del sistema es mayor que la condición definida previamente. Si un suceso coincide con un filtro de sucesos y usted ha configurado este filtro para que genere una alerta (alerta de correo electrónico o captura de SNMP), se envía una alerta a los destinos configurados.

Para configurar la CMC para enviar alertas:

1. Active las alertas de sucesos globales del chasis.
2. De forma opcional, puede seleccionar los sucesos para los cuales se deben generar alertas.
3. Configure los valores de la alerta por correo electrónico o la captura SNMP.
4. Active el Registro mejorado del chasis.

Conceptos relacionados

Activación o desactivación de alertas en la página 126
Configuración de destinos de alerta en la página 127

Temas:

Activación o desactivación de alertas

Para enviar alertas a los destinos configurados, debe activar la opción de alertas globales. Esta propiedad anula la configuración de las alertas individuales.

Asegúrese de que el SNMP o los destinos de alerta por correo electrónico estén configurados para recibir las alertas.

Activación o desactivación de alertas mediante la interfaz web del CMC

Para activar o desactivar la generación de alertas:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Alertas** > **Sucesos del chasis**. Aparecerá la página **Sucesos del chasis**.
2. En la sección **Configuración de filtros de sucesos del chasis**, seleccione la opción **Activar alertas de sucesos del chasis** para activar la generación de alertas. Para desactivar la generación de alertas, desmarque esta opción.
3. En la sección **Lista de sucesos del chasis**, realice una de las siguientes operaciones:
   - Seleccione sucesos individuales para los que se deben generar alertas.
   - Seleccione la opción **Enable Alert (Activar alerta)** en el encabezado de columna para generar alertas para todos los sucesos. De lo contrario, elimine la selección.
4. Haga clic en **Aplicar** para guardar la configuración.

Activación o desactivación de alertas mediante RACADM

Para activar o desactivar la generación de alertas, use el objeto de RACADM `cfgAlertingEnable`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

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**.

Conceptos relacionados

Configuración de destinos de alerta de las capturas SNMP en la página 127
Configuración de los valores de alertas por correo electrónico en la página 129

Configuración de destinos de alerta de las capturas SNMP

Es posible configurar las direcciones IPv6 o IPv4 para la recepción de capturas SNMP.

Configuración de destinos de alerta de las capturas SNMP mediante la interfaz web del CMC

Para configurar los valores de destino de alerta IPv4 o IPv6 mediante la interfaz web del CMC:

1. En el 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 **Destination (Destino)**, introduzca una dirección IP válida. Utilice el formato IPv4 de cuatro números con puntos intermedios, la notación de dirección IPv6 estándar o FQDN. Por ejemplo: `123.123.123.123`, `2001:db8:85a3::8a2e:370:7334` o `dell.com`.

     Elija un formato que guarde coherencia con la infraestructura o la tecnología de la red. La función Test Trap (Probar captura) no puede detectar las selecciones incorrectas en función de la configuración de red actual (por ejemplo, el uso de un destino IPv6 en un entorno exclusivamente 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 a la que se muestra en la página **Chassis (Chasis)** > **Network (Red)** > **Services (Servicios)**. La cadena de comunidad de capturas SNMP es la comunidad que la CMC utiliza para las capturas salientes destinadas a estaciones de administración. La cadena de comunidad de la página **Chassis (Chasis)** > **Network (Red)** > **Services (Servicios)** es la cadena de comunidad que las estaciones de administración utilizan para consultar el demonio 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 **Enabled (Activada)**, seleccione la casilla de verificación correspondiente a la IP de destino para activar en la dirección IP la recepción de 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: Se puede seleccionar una sola máscara de filtro para las alertas tanto de SNMP como por correo electrónico. Puede saltear 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. Especifique los sucesos para los que se deben generar alertas:

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

donde `<mask value>` es un valor hexadecimal entre 0x0 y 0xffffffff.

Para obtener el valor de la máscara, utilice una calculadora científica en modo hexadecimal y sume los segundos valores de las máscaras individuales (1, 2, 4, etc.) utilizando la tecla <O>.

Por ejemplo, para activar las alertas de captura para la advertencia de sonda de baterías (0x2), la falla del suministro de energía (0x1000) y la falla del KVM (0x80000), ingrese 2 <O> 1000 <O> 200000 y presione la tecla <=>.

El valor hexadecimal resultante es 81002, y el valor de la máscara para el comando RACADM es 0x81002.

Tabla 19. Máscaras de filtro para capturas de sucesos

Suceso	Valor de la máscara de filtro
Falla de sonda del ventilador	0x1
Aviso de sonda de baterías	0x2
Aviso de sonda de temperatura	0x8
Falla de sonda de temperatura	0x10
Redundancia degradada	0x40
Redundancia perdida	0x80
Aviso del suministro de energía	0x800
Falla del suministro de energía	0x1000
Suministro de energía ausente	0x2000
Falla de registro de hardware	0x4000
Aviso del registro de hardware	0x8000
Servidor ausente	0x10000
Falla del servidor	0x20000
KVM ausente	0x40000
Falla del KVM	0x80000
Módulo de E/S ausente	0x100000
Falla del módulo de E/S	0x200000
Incompatibilidad de versión del firmware	0x400000
Error del umbral de alimentación del chasis	0x1000000
Tarjeta SD ausente	0x2000000
Error en la tarjeta SD	0x4000000
Error del grupo de chasis	0x8000000
Alojamiento del servidor ausente	0x10000000
Incompatibilidad con la red Fabric	0x20000000

4. 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 completos (FQDN).

5. Especifique una dirección IP de destino para recibir la alerta de capturas:

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
```

donde <IP address> es un destino válido, y <index> es el valor de índice especificado en el paso 4.

6. Especifique el nombre de comunidad:

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i <index>
```

donde <community name> es la comunidad SNMP a la que pertenece el chasis e <index> es el valor de índice especificado 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 6.

NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgTraps -i <index>`. Si el índice está configurado, aparecerán los valores para los objetos `cfgTrapsAlertDestIPAddr` y `cfgTrapsCommunityName`.

7. Para probar cuál es el destino de las alertas de una captura de sucesos, escriba:

```
racadm testtrap -i <index>
```

donde <index> es un valor de 1 a 4 que representa el destino de alertas 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 alertas por correo electrónico

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

Debe configurar el servidor de correo electrónico SMTP para que acepte correos electrónicos retransmitidos desde 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 para hacer esto de forma segura, consulte la documentación incluida con el servidor SMTP.

NOTA: Si el servidor de correo es Microsoft Exchange Server 2007, compruebe que el nombre de dominio de iDRAC está configurado para que el servidor de correo reciba alertas por correo electrónico desde iDRAC.

NOTA: Las alertas por correo electrónico admiten direcciones IPv4 e IPv6. El nombre de dominio DNS de DRAC se debe especificar al utilizar IPv6.

Si su red tiene un servidor SMTP que envía y renueva 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 IP especificada del servidor SMTP. En estos casos, use el nombre DNS.

Configuración de los valores de alerta por correo electrónico mediante la interfaz web del CMC

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

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Alertas** > **Valores de alerta de correo electrónico**.
2. Especifique los valores para el servidor de correo electrónico SMTP y las direcciones de correo electrónico donde se deben recibir las alertas. Para obtener información acerca de los campos, consulte *CMC Online Help (Ayuda en línea de 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 por correo electrónico mediante RACADM:

1. Abra una consola de texto de serie/Telnet/SSH en la CMC e inicie sesión.
2. Active la generación de alertas:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

NOTA: Se puede seleccionar una sola máscara de filtro para las alertas tanto de SNMP como por correo electrónico. Puede saltear el paso 3 si ya ha seleccionado una máscara de filtro.

3. Especifique los sucesos para los que se deben generar alertas:

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

donde `<mask value>` es un valor hexadecimal entre 0x0 y 0xffffffff, y debe expresarse con la caracteres iniciales 0x. La tabla Máscaras de filtro para capturas de sucesos proporciona máscaras de filtro para cada tipo de suceso. Para obtener instrucciones para calcular el valor hexadecimal de la máscara de filtro que desea activar, consulte el paso 3 en Configuración de destinos de alerta de las capturas SNMP mediante RACADM.

4. Active la generación de alertas por correo electrónico:

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

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

5. Especifique una dirección de correo electrónico de destino para recibir las alertas por correo electrónico:

```
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 de índice especificado en el paso 4.

6. Especifique el nombre de la persona que recibirá la alerta por correo electrónico:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i <index>
```

donde `<email name>` es el nombre de la persona o el grupo que recibe la alerta por correo electrónico, e `<index>` es el valor de índice especificado en los pasos 4 y 5. El nombre de correo electrónico puede contener hasta 32 caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.

7. Configure el host SMTP:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
```

donde `host.domain` es el nombre de dominio completo.

Puede configurar hasta cuatro direcciones de correo electrónico de destino para recibir alertas por correo electrónico. Para agregar más direcciones, repita los pasos 2 a 6.

NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice 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 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

9

Configuración de cuentas de usuario y privilegios

Puede configurar las cuentas de usuario con privilegios específicos (*autoridad basada en funciones*) para administrar el sistema con la CMC y mantener la seguridad del sistema. De manera predeterminada, la CMC viene configurada con una cuenta de administrador local. El nombre de usuario predeterminado es *root* y la contraseña predeterminada es *calvin*. Como administrador, puede configurar cuentas de usuario para permitir a otros usuarios acceder a la CMC.

Puede configurar hasta 16 usuarios locales o utilizar servicios de directorio, como Microsoft Active Directory o LDAP, para configurar cuentas de usuario adicionales. El uso de un servicio de directorio proporciona una ubicación central para administrar las cuentas de usuario autorizadas.

La CMC admite el acceso basado en funciones para los usuarios con un conjunto de privilegios asociados. Las funciones son administrador, operador, solo lectura o ninguna. La función define los privilegios máximos disponibles.

Conceptos relacionados

Tipos de usuarios en la página 131
Configuración de usuarios locales en la página 135
Configuración de usuarios de Active Directory en la página 137
Configuración de los usuarios LDAP genéricos en la página 151

Tareas relacionadas

Modificación de la configuración de cuentas raíz de administración para usuarios en la página 134

Temas:

Tipos de usuarios

Hay dos tipos de usuarios:

- Usuarios de la CMC o usuarios del chasis
- Usuarios del iDRAC o usuarios del servidor (dado que el iDRAC reside en un servidor)

Los usuarios del iDRAC y de la CMC pueden ser usuarios locales o usuarios del servicio de directorio.

Excepto cuando un usuario de la CMC tiene privilegios de **Administrador de servidor**, los privilegios otorgados a un usuario de la CMC no se transfieren automáticamente al mismo usuario en un servidor, ya que los usuarios de servidores se crean independientemente de los usuarios de la CMC. En otras palabras, los usuarios de Active Directory de la CMC y los usuarios de Active Directory de la iDRAC residen en dos ramas diferentes del árbol de Active Directory. Para crear un usuario de servidor local, los usuarios de configuración deben iniciar sesión directamente en el servidor. Los usuarios de configuración no pueden crear un usuario de servidor desde la CMC ni viceversa. Esta regla protege la seguridad y la integridad de los servidores.

Tabla 20. Tipos de usuarios

Privilegio	Descripción
Usuario con acceso a la CMC	El usuario puede iniciar sesión en la CMC y ver todos los datos de la CMC, pero no puede agregar o modificar datos ni ejecutar comandos.

Tabla 20. Tipos de usuarios (continuación)

Privilegio	Descripción
	Es posible que un usuario tenga otros privilegios, pero no tenga el privilegio de Usuario con acceso a la CMC. Esta función es útil cuando temporalmente a un usuario no se le permite iniciar sesión. 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. ● Se relacionan con el chasis, como el nombre de ranura y la prioridad de ranura. Si bien estas propiedades se aplican a los servidores, se trata estrictamente de propiedades del chasis que se relacionan con las ranuras y no con los servidores en sí mismos. Por este motivo, los nombres de ranura y las prioridades de ranura se pueden agregar o cambiar sin importar si hay servidores presentes en las ranuras o no. Cuando se mueve un servidor a un chasis diferente, este hereda el nombre y la prioridad asignados a la ranura que ocupa en el chasis nuevo. Su prioridad y nombre de ranura anteriores se conservarán en el chasis anterior. **NOTA:** Los usuarios de la CMC con el privilegio de **Administrador de configuración del chasis** pueden configurar los valores de alimentación. Sin embargo, el privilegio de **Administrador de control del chasis** es necesario para las 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 del usuario y otros privilegios 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 con el privilegio de **Administrador de alimentación del chasis** pueden llevar a cabo todas las operaciones relativas a la alimentación. Pueden controlar las operaciones de alimentación del chasis, como 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 de 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. En otras palabras, el privilegio de **Administrador de 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 sin privilegio de **Administrador de servidor** genera una acción que se debe realizar en un servidor, la CMC envía un comando al servidor de destino con el nombre y la contraseña del usuario. Si el usuario no existe en el servidor o si la contraseña no coincide, no se permite al usuario ejecutar la acción.

Tabla 20. Tipos de usuarios (continuación)

Privilegio	Descripción
	Si el usuario existe en el servidor de destino y la contraseña coincide, el servidor responde con los privilegios que el usuario tiene en el servidor. En función de los privilegios que indique la respuesta del servidor, el firmware de la CMC decide si el usuario tiene derecho a ejecutar la acción.
	A continuación se muestra una lista de los privilegios y las acciones en el servidor a las que tiene derecho el Administrador de servidor. Estos derechos se aplican solamente cuando el usuario del chasis no tiene el privilegio administrativo del servidor en el chasis. Administrador de configuración del servidor: ● Establecer dirección IP ● Establecer puerta de enlace ● Establecer máscara de subred ● Establecer primer dispositivo de inicio Configurar usuarios: ● Establecer contraseña raíz del iDRAC ● Restablecimiento de iDRAC Administrador de control del servidor: ● Encendido ● Apagado ● Ciclo de encendido ● Apagado ordenado ● Reinicio del servidor
Usuario de alertas de prueba	El usuario puede enviar mensajes de alerta de prueba.
Administrador de comandos de depuración	El usuario puede ejecutar comandos de diagnóstico del sistema.
Administrador de red Fabric A	El usuario puede definir y configurar el módulo de E/S de la red Fabric A, que reside en la ranura A1 o en la ranura A2 de las ranuras de E/S.
Administrador de red Fabric B	El usuario puede definir y configurar el módulo de E/S de la red Fabric B, que reside en la ranura B1 o en la ranura B2 de las ranuras de E/S.
Administrador de red Fabric C	El usuario puede definir y configurar el módulo de E/S de la red Fabric C, que reside en la ranura C1 o en la ranura C2 de las ranuras de E/S.

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 21. Privilegios del grupo de la CMC

Grupo de usuarios	Privilegios otorgados
Administrador	● Usuario con acceso a la CMC ● Administrador de configuración del chasis ● Administrador de configuración de usuarios ● Administrador de borrado de registros ● Administrador del servidor ● Usuario de alertas de prueba ● Administrador de comandos de depuración ● Administrador de red Fabric A ● Administrador de red Fabric B ● Administrador de red Fabric C
Usuario avanzado	● Inicio de sesión

Tabla 21. Privilegios del grupo de la CMC (continuación)

Grupo de usuarios	Privilegios otorgados
	• 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 • Administrador de red Fabric B • Administrador de red Fabric C
Usuario invitado	Inicio de sesión
Personalizado	Seleccione cualquier combinación de los siguientes permisos: • Usuario con acceso a la CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Administrador del servidor • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A • Administrador de red Fabric B • Administrador de red Fabric C
Ninguno	Sin permisos asignados

Tabla 22. Comparación de los privilegios entre administradores, usuarios avanzados y usuarios invitados de la CMC

Conjunto de privilegios	Permisos de administrador	Permisos de usuario avanzado	Permisos de usuario invitado
Usuario con acceso a la CMC	Sí	Sí	Sí
Administrador de configuración del chasis	Sí	No	No
Administrador de configuración de usuarios	Sí	No	No
Administrador de borrado de registros	Sí	Sí	No
Administrador de control del chasis (comandos de alimentación)	Sí	Sí	No
Administrador del servidor	Sí	Sí	No
Usuario de alertas de prueba	Sí	Sí	No
Administrador de comandos de depuración	Sí	No	No
Administrador de red Fabric A	Sí	Sí	No
Administrador de red Fabric B	Sí	Sí	No
Administrador de red Fabric C	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 el CMC.

Para cambiar la contraseña predeterminada para la cuenta raíz mediante la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Descripción general del chasis** y haga clic en **Autentificación de usuario** > **Usuarios locales**.
   Se muestra la página **Users (Usuarios)**.
2. En la columna **Identificación de usuario**, haga clic en la identificación de usuario 1.

   NOTA: Identificación de usuario 1 es la cuenta de usuario raíz que se envía con el CMC. Este valor no se puede modificar.

   Aparecerá la página **User Configuration (Configuración de usuario)**.
3. Seleccione la casilla **Cambiar contraseña**.
4. Escriba la nueva contraseña en los campos **Contraseña** y **Confirmar contraseña**.
5. Haga clic en **Aplicar**.
   Se cambiará la contraseña para la identificación de usuario 1.

Configuración de usuarios locales

Puede configurar hasta 16 usuarios locales en la CMC con permisos de acceso específicos. Antes de crear un usuario local para la CMC, verifique si ya existen usuarios. Puede establecer los nombres de usuario, las contraseñas y las funciones con los privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar mediante cualquiera de las interfaces seguras de la CMC (es decir, la interfaz web, RACADM o WS-MAN).

Configuración de los usuarios locales con la interfaz web del CMC

Para agregar y configurar usuarios locales en la CMC:

NOTA: Es necesario contar con el permiso **Configurar usuarios** para poder crear un usuario de la CMC.

1. En el árbol del sistema, diríjase a **Descripción general del chasis** y haga clic en **Autentificación de usuario** > **Usuarios locales**.
   Se muestra la página **Users (Usuarios)**.
2. En la columna **User ID (Id. de usuario)**, haga clic en un número de Id. de usuario.

   NOTA: Identificación de usuario 1 es la cuenta de usuario raíz que se envía con el CMC. Este valor no se puede modificar.

   Aparecerá la página **User Configuration (Configuración de usuario)**.
3. Active la identificación de usuario y especifique el nombre de usuario, la contraseña y los privilegios de acceso de usuario.
   Para obtener más información acerca de estas opciones, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
4. Haga clic en **Aplicar**.
   El usuario se crea con los privilegios necesarios.

Configuración de los usuarios locales mediante RACADM

NOTA: Se debe haber iniciado sesión como usuario **root** para ejecutar los comandos de RACADM en un sistema remoto con Linux.

Puede configurar hasta 16 usuarios en la base de datos de propiedades de la CMC. Antes de activar manualmente a un usuario de la CMC, verifique si ya existe algún usuario.

Si va a configurar una CMC nueva o ha utilizado el comando racadm `racresetcfg`, el único usuario actual es `root` con la contraseña `calvin`. El subcomando `racresetcfg` restablece todos los parámetros de configuración predeterminados originales. 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 el 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 ningún valor, ese número de índice, indicado por el objeto `cfgUserAdminIndex`, se puede usar. Si se muestra un nombre después del signo "=", ese índice lo lleva ese nombre de usuario.

Cuando activa o desactiva manualmente un usuario con el subcomando racadm `config` , **debe** especificar el índice con la opción `-i`.

El carácter "#" en los objetos de comando indica que se trata de un objeto de solo lectura. Asimismo, si utiliza el comando `racadm config -f racadm.cfg` para especificar cualquier número de grupos u objetos para escritura, el índice no se puede especificar. Los nuevos usuarios se agregan al primer índice disponible. Este comportamiento permite una mayor flexibilidad a la hora de configurar una segunda CMC con la misma configuración que la CMC principal.

Adición de un usuario del CMC mediante RACADM

Para agregar un nuevo usuario a la configuración del CMC, realice los pasos siguientes:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca los privilegios de usuario. Para obtener información sobre los privilegios de usuario, consulte Tipos de usuarios.
4. Active el usuario.

Por ejemplo:

En el siguiente ejemplo se describe la forma de agregar un nuevo usuario de nombre "John" con la contraseña "123456" y privilegios de inicio de sesión en el CMC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2
john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2
123456
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege
0x00000001
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

NOTA: Consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)* para obtener una lista de valores de máscara de bits válidos para determinados privilegios de usuario. El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene activado ningún privilegio.

Para verificar que el usuario se haya agregado correctamente con los privilegios correctos, use uno de los siguientes comandos:

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

Para obtener más información acerca de los comandos RACADM, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

Desactivación de un usuario del CMC

Al usar RACADM, los usuarios se deben desactivar manualmente y de manera individual. Los usuarios no se pueden eliminar mediante un archivo de configuración.

Para eliminar un usuario del CMC, la sintaxis de comando es:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <index>""
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x0
```

Una cadena nula de dos caracteres de comillas ("") indica al CMC que debe eliminar la configuración de usuario en el índice especificado y restablecer los valores predeterminados originales de fábrica en la configuración de usuario.

Activación de un usuario del CMC con permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en funciones):

1. Busque un índice de usuario disponible mediante la sintaxis de comando siguiente:

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

2. Escriba los comandos siguientes con el nombre de usuario y la contraseñas nuevos.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <index> <user privilege bitmask value>
```

NOTA: Para ver una lista de los valores de máscara de bits válidos para privilegios de usuario específicos, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)* en **dell.com/support/manuals**. El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene activado ningún privilegio.

Configuración de usuarios de Active Directory

Si su empresa utiliza el software Microsoft Active Directory, puede configurar el software para brindar acceso a la CMC, y puede 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: El uso de Active Directory para reconocer usuarios de la CMC se admite en los sistemas operativos Microsoft Windows 2000 y Windows Server 2003. Active Directory a través de IPv6 e IPv4 se admite en Windows 2008.

Puede configurar la autentificación de usuarios a través de Active Directory para iniciar sesión en la CMC. También puede ofrecer autoridad basada en funciones, que permite al administrador configurar 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.
- La 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 máxima flexibilidad a la hora de configurar el acceso de usuario en distintas CMC con niveles de privilegios variados.

Conceptos relacionados

Descripción general del esquema estándar de Active Directory en la página 137
Descripción general del esquema extendido de Active Directory en la página 140

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.

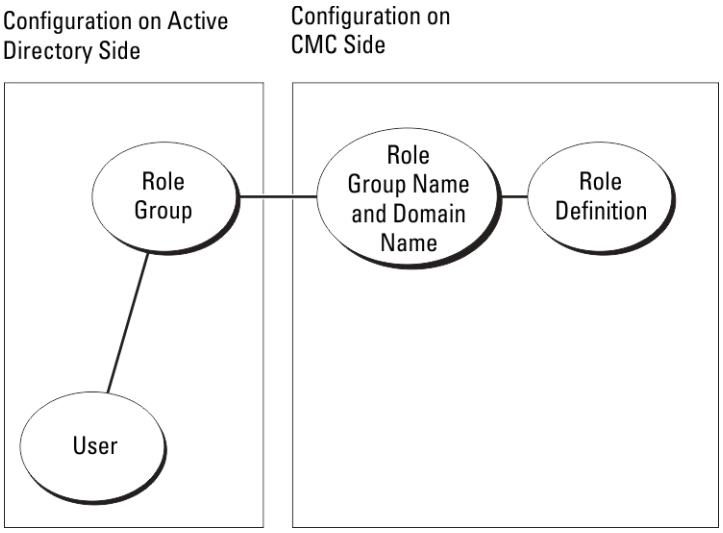


Ilustración 7. Configuración de la CMC con el esquema estándar de Active Directory

En Active Directory, se utiliza como grupo de funciones un objeto de grupo estándar. 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 privilegios se definen en cada tarjeta CMC y no en Active Directory. Puede configurar hasta cinco grupos de funciones en cada CMC. En la siguiente tabla se presentan los privilegios predeterminados de los grupos de funciones.

Tabla 23. : Privilegios predeterminados del grupo de funciones

Grupo de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
1	Ninguno	• Usuario con acceso a la CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Administrador del servidor • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A • Administrador de red Fabric B • Administrador de red Fabric C	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 • Administrador de red Fabric B • Administrador de red Fabric C	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 el CMC para un acceso de inicio de sesión de Active Directory:

1. En un servidor de Active Directory (controladora de dominio), abra **Active Directory Users and Computers Snap-in (Complemento Usuarios y equipos de Active Directory)**.
2. Mediante la interfaz web de la CMC o RACADM:
   a. Cree un grupo o seleccione un grupo existente.
   b. Configure los privilegios de funciones.
3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para obtener acceso a la CMC.

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

NOTA: Para obtener información acerca de los distintos campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

1. En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **User Authentication (Autentificación de usuario)** > **Directory Services (Servicios de directorio)**. Aparecerá la página **Directory Services (Servicios de directorio)**.
2. Seleccione **Microsoft Active Directory (Esquema estándar)**. Los valores que se deben configurar para el esquema estándar se mostrarán en la misma página.
3. Especifique lo siguiente:
   - Habilite Active Directory, introduzca el nombre de dominio raíz y el valor de tiempo de espera.
   - Si desea que la llamada dirigida realice una búsqueda en la controladora de dominio y el catálogo global, seleccione la opción **Buscar servidor de AD para la búsqueda (opcional)** y especifique los detalles de la controladora de dominio y el catálogo global.
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 **Standard Schema Settings (Configuración de esquema estándar)**, haga clic en un **Role Group (Grupo de funciones)**. Aparecerá la página **Configure Role Group (Configurar grupo de funciones)**.
6. Especifique el nombre del grupo, el dominio y los privilegios para el grupo de funciones.
7. Haga clic en **Aplicar** para guardar la configuración del grupo de funciones y haga clic en **Volver a la página de configuración**.
8. Si ha activado la validación de certificados, debe cargar en el CMC el certificado firmado por una autoridad de certificados raíz para el bosque de dominio. En la sección **Administrar certificados**, escriba la ruta de acceso del archivo o busque el archivo de certificado. Haga clic en **Cargar** para cargar el archivo en el CMC.

   NOTA: El valor **File Path (Ruta de acceso del archivo)** muestra la ruta de acceso relativa del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso absoluta del archivo, que incluye la ruta de acceso completa más el nombre completo del archivo con la extensión.

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

9. Si ha activado el inicio de sesión único (SSO), en la sección **Kerberos Keytab (Archivo keytab de Kerberos)**, haga clic en **Browse (Examinar)**, especifique el archivo keytab y, a continuación, haga clic en **Upload (Cargar)**. Al completarse la carga, aparecerá un mensaje que indica que la carga ha sido correcta o ha fallado.
10. Haga clic en **Aplicar**. El servidor web de la CMC se reiniciará automáticamente al hacer clic en **Apply (Aplicar)**.
11. Cierre sesión y luego inicie sesión en el CMC para completar la configuración de Active Directory en el CMC.
12. Seleccione **Chassis (Chasis)** en el árbol del sistema y desplácese hasta la ficha **Network (Red)**. Aparecerá la página **Configuración de la red**.
13. En **Configuración de la red**, si la opción **Usar DHCP (para la dirección IP de la interfaz de red del CMC)** está seleccionada, seleccione **Usar DHCP para obtener dirección de servidor DNS**.

Para introducir manualmente una dirección IP de servidor DNS, desactive **Use DHCP to obtain DNS server addresses (Usar DHCP para obtener direcciones de servidor DNS)** y escriba las direcciones IP del servidor DNS principal y alternativo.

14. Haga clic en **Aplicar cambios**.

    De esta forma, se completa la configuración de la función de Active Directory de esquema estándar para el CMC.

Configuración de Active Directory con esquema estándar vía RACADM

Para configurar Active Directory en el CMC con esquema estándar mediante RACADM:

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <fully qualified root domain name>
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupName <common name of the role
group>
racadm config -g cfgStandardSchema -i <index>-o
cfgSSADRoleGroupDomain <fully qualified domain
name>
racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Bit mask number for
specific user permissions>
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate>
racadm sslcertdownload -t 0x1 -f <RAC SSL
certificate>
```

   NOTA: Para ver los valores de los números de la máscara de bits, consulte el capítulo de propiedades de la base de datos de *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

2. Especifique un servidor DNS por medio de una de las siguientes opciones:
   - Si DHCP está activado en el CMC y desea utilizar la dirección de DNS obtenida automáticamente mediante el servidor DHCP, escriba el siguiente comando:

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

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

     ```
     racadm config -g cfgLanNetworking -o
     cfgDNSServersFromDHCP 0
     racadm config -g cfgLanNetworking -o
     cfgDNSServer1 <primary DNS IP address>
     racadm config -g cfgLanNetworking -o
     cfgDNSServer2 <secondary DNS IP address>
     ```

Descripción general del esquema extendido de Active Directory

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

Extensiones de esquema de Active Directory

Los datos de Active Directory son una base de datos distribuida de *atributos* y *clases*. El esquema de Active Directory incluye las reglas que determinan los tipos de datos que se pueden agregar o incluir en la base de datos. Un ejemplo de una clase que se almacena en la base de datos es la clase usuario. Algunos ejemplos de los atributos de la clase usuario pueden ser el nombre, el apellido, el número de teléfono, etc.

Puede ampliar la base de datos de Active Directory añadiendo sus propios *atributos* y *clases* exclusivos para satisfacer requisitos específicos. Dell ha extendido el esquema para incluir los cambios necesarios a fin de admitir la autorización y la autentificación de administración remota mediante Active Directory.

Cada *atributo* o *clase* que se agrega a un esquema de Active Directory debe definirse con una Id. exclusiva. Para que no se repitan en toda la industria, Microsoft mantiene una base de datos de identificadores de objetos de Active Directory (OID), de modo que, cuando las empresas agregan extensiones al esquema, pueden tener la garantía de que serán exclusivos y no entrarán en conflicto entre sí. Para extender el esquema en Microsoft Active Directory, Dell recibe OID, extensiones de nombre e Id. de atributos con vínculos exclusivos para los atributos y las clases que se agregan al servicio de directorio.

- Extensión de Dell: `dell`
- OID básico de Dell: `1.2.840.113556.1.8000.1280`
- Rango de LinkID del RAC: `12070 a 12079`

Descripción general sobre las extensiones de esquema

Dell ha extendido el esquema para incluir una propiedad *Asociación*, *Dispositivo* y *Privilegio*. La propiedad *Asociación* se utiliza para vincular a los usuarios o grupos de un conjunto específico de privilegios con uno o varios dispositivos de RAC. Este modelo proporciona al administrador la máxima flexibilidad para las distintas combinaciones de usuarios, privilegios de RAC y dispositivos de RAC en la red sin demasiada complejidad.

Si existen dos CMC en la red que se desean integrar a Active Directory para autentificación y autorización, es necesario crear al menos un objeto de asociación y un objeto de dispositivo de RAC para cada CMC. Es posible crear varios objetos de asociación, y cada objeto de asociación puede vincularse a la cantidad de usuarios, grupos de usuarios u objetos de dispositivo de RAC que sea necesaria. Los usuarios y los objetos de dispositivo de RAC pueden ser miembros de cualquier dominio de la empresa.

Sin embargo, cada objeto de asociación se puede vincular (o puede vincular usuarios, grupos de usuarios u objetos de dispositivo de RAC) a un solo objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en CMC específicas.

El objeto de dispositivo de RAC es el vínculo con el firmware de RAC para consultar a Active Directory con fines de autentificación y autorización. Cuando se agrega un RAC a la red, el administrador debe configurar el RAC y su objeto de dispositivo con el nombre de Active Directory, de modo que los usuarios puedan realizar la autentificación y la autorización con Active Directory. Además, el administrador debe agregar el RAC a por lo menos un objeto de asociación para que los usuarios se puedan autentificar.

En la figura siguiente se muestra que el objeto de asociación proporciona la conexión necesaria para la autentificación y la autorización.

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

Puede crear la cantidad de objetos de asociación que sea necesaria. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo de RAC para cada RAC (CMC) de la red que desee integrar con Active Directory.

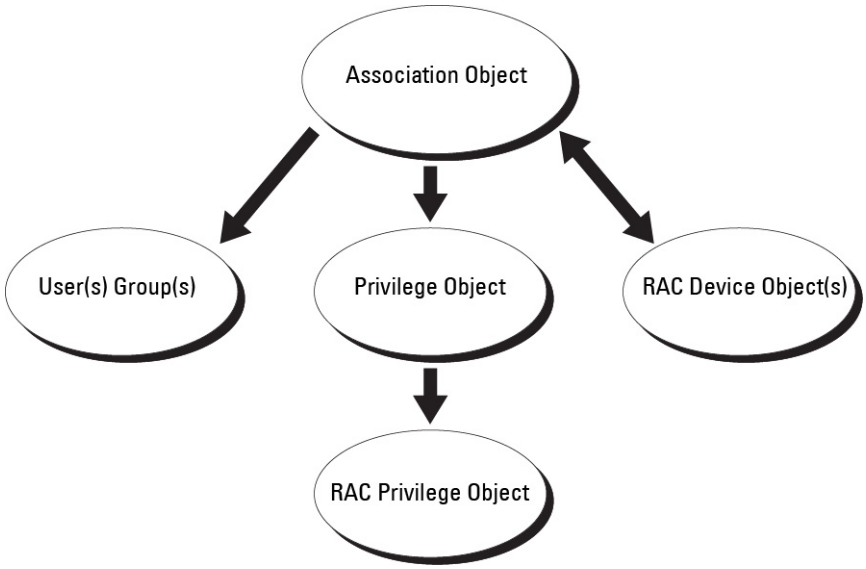


Ilustración 8. Configuración típica de los objetos de Active Directory

El objeto de asociación le permite tener la cantidad que desee de usuarios o grupos y objetos de dispositivo de RAC. No obstante, el objeto de asociación solo incluye un objeto de privilegio por objeto de asociación. El objeto de asociación conecta a los *usuarios* que tienen *privilegios* en los RAC (CMC).

Además, se puede configurar objetos de Active Directory en un solo dominio o en varios. Por ejemplo, puede tener dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory (usuario1, usuario2 y usuario3). Quizás desee otorgar el privilegio de administrador para ambas

CMC al usuario1 y al usuario2, y el privilegio de inicio de sesión en la tarjeta de RAC2 al usuario3. En la siguiente figura se muestra la forma de configurar los objetos de Active Directory en este escenario.

Al agregar grupos universales desde dominios independientes, cree un objeto de asociación con ámbito universal. Los objetos de asociación predeterminados que crea la utilidad Dell Schema Extender son grupos locales de dominios y no funcionan con grupos universales de otros dominios.

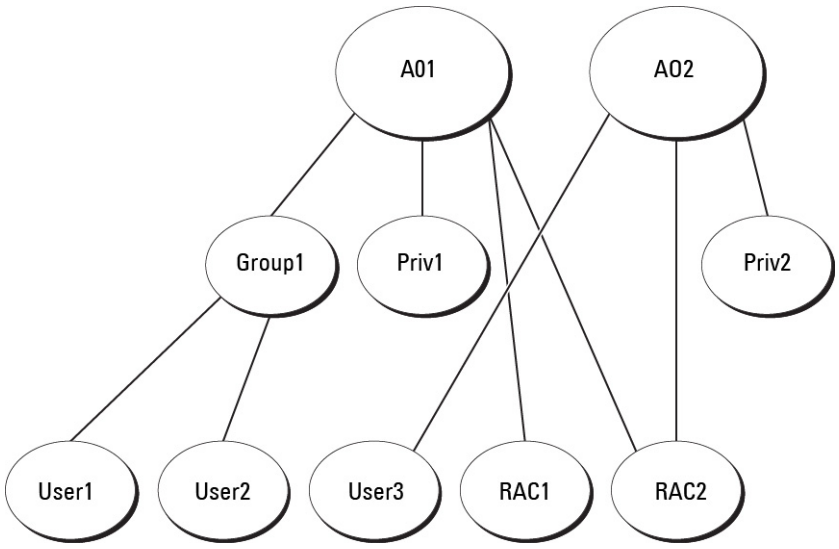


Ilustración 9. Configuración de objetos de Active Directory en un solo dominio

Para configurar los objetos en un escenario de un solo dominio:

1. Cree dos objetos de asociación.
2. Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representen a los dos CMC.
3. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tenga todos los privilegios (de administrador) y Priv2 tenga el privilegio de inicio de sesión.
4. Agrupe usuario1 y usuario2 en grupo1.
5. Agregue Group1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objeto de privilegio en A01, y RAC1 y RAC2 como dispositivos de RAC en A01.
6. Agregue User3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objeto de privilegio en A02, y RAC2 como dispositivo de RAC en A02.

En la siguiente figura se muestra un ejemplo de objetos de Active Directory en varios dominios. En este escenario, tiene dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory (usuario1, usuario2 y usuario3). El usuario1 está en el dominio1, y el usuario2 y el usuario 3 están en el dominio2. En este escenario, configure privilegios de administrador en ambas CMC para el usuario1 y el usuario2, y privilegios de inicio de sesión en la tarjeta de RAC2 para el usuario3.

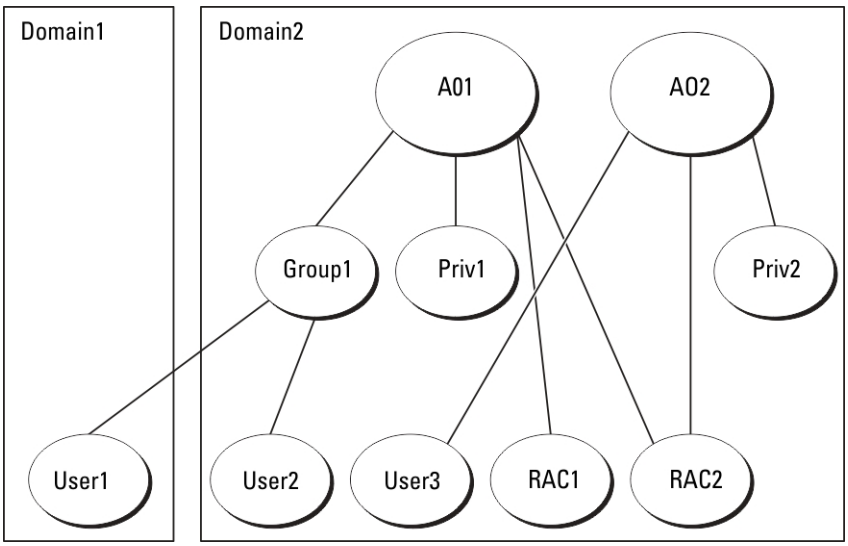


Ilustración 10. Configuración de objetos de Active Directory en varios dominios

Para configurar los objetos en un escenario de varios dominios:

1. Asegúrese de que la función de bosque del dominio esté en el modo Nativo o Windows 2003.
2. Cree dos objetos de asociación, A01 (de ámbito universal) y A02, en cualquier dominio. En la figura Configuración de objetos de Active Directory en varios dominios, se muestran los objetos en el dominio2.
3. Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representen a los dos CMC.
4. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tenga todos los privilegios (de administrador) y Priv2 tenga el privilegio de inicio de sesión.
5. Agrupe usuario1 y usuario2 en grupo1. El ámbito del grupo1 debe ser universal.
6. Agregue Group1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objeto de privilegio en A01, y RAC1 y RAC2 como dispositivos de RAC en A01.
7. Agregue User3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objeto de privilegio en A02, y RAC2 como dispositivo de RAC en A02.

Configuración del esquema extendido de Active Directory

Para configurar Active Directory para obtener acceso a la CMC:

1. Amplíe el esquema de Active Directory.
2. Amplíe el complemento Usuarios y equipos de Active Directory.
3. Agregue usuarios de la CMC y sus privilegios en Active Directory.
4. Active SSL en cada una de las controladoras de dominio.
5. Configure las propiedades de Active Directory para el CMC mediante la interfaz web del CMC o de RACADM.

Conceptos relacionados

Extensión del esquema de Active Directory en la página 143
Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory en la página 147
Agregar usuarios y privilegios del CMC a Active Directory en la página 147

Tareas relacionadas

Configuración de Active Directory con esquema extendido mediante la interfaz web del CMC en la página 149
Configuración de Active Directory con esquema extendido mediante RACADM en la página 150

Extensión del esquema de Active Directory

Al extender el esquema de Active Directory se le agrega una unidad organizacional de Dell, clases y atributos de esquema, y privilegios y objetos de asociación de ejemplo. Antes de extender el esquema, debe asegurarse de tener privilegios de administrador de esquema en el propietario del rol de operaciones de maestro único flexible (FSMO) de maestro de esquema en el bosque de dominio.

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

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

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

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation (Herramientas y documentación de Dell Systems Management)*, en los siguientes directorios respectivos:

- `DVDdrive:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management\LDIF_Files`
- `<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management\Schema Extender`

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que se incluye en el directorio `LDIF_Files`.

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

Uso de Dell Schema Extender

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

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

   El esquema ya está extendido. Para revisar la extensión del esquema, utilice la MMC y el complemento de esquema de Active Directory para verificar que las clases y los atributos existan. Para obtener más información sobre las clases y los atributos, consulte Clases y atributos. Consulte la documentación de Microsoft para ver detalles acerca del uso de la MMC y el complemento de esquema de Active Directory.

Clases y atributos

Tabla 24. : Definiciones de clases para las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 25. : Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo de RAC Dell. El RAC debe configurarse como delliDRACDevice en Active Directory. Esta configuración permite que la CMC envíe consultas de protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 26. : Clase delliDRACAssociationObject

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Grupo
Atributos	dellProductMembers dellPrivilegeMember

Tabla 27. : Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (derechos de autorización) para el dispositivo CMC.

Tabla 27. : Clase dellRAC4Privileges (continuación)

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tabla 28. : Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	Usuario
Atributos	dellRAC4Privileges

Tabla 29. : Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	dellAssociationMembers

Tabla 30. : Lista de atributos agregados al esquema de Active Directory

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Atributo: `dellPrivilegeMember` **Descripción**: Lista de objetos `dellPrivilege` que pertenecen a este atributo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.1 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellProductMembers` **Descripción**: Lista de objetos `dellRacDevices` que pertenecen a este rol. Este atributo es el vínculo de avance para el vínculo de retroceso `dellAssociationMembers`. **Identificación de vínculo**: 12070 **OID**: 1.2.840.113556.1.8000.1280.1.1.2.2 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellIsCardConfigAdmin`	VERDADERO

Tabla 30. : Lista de atributos agregados al esquema de Active Directory (continuación)

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Descripción: el valor es VERDADERO si el usuario tiene derechos de configuración de tarjeta en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Atributo: `dellIsLoginUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de inicio de sesión en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsUserConfigAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de configuración de usuario en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsLogClearAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de borrado de registros en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsServerResetUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos para restablecer el servidor en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsTestAlertUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de usuario de alertas de prueba en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsDebugCommandAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de comandos de depuración en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellSchemaVersion` **Descripción**: se utiliza la versión de esquema actual para actualizar el esquema. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.12 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
Atributo: `dellRacType` **Descripción**: este atributo representa el tipo de RAC actual para el objeto dellRacDevice y el vínculo de retroceso al vínculo de avance dellAssociationObjectMembers. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.13 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO

Tabla 30. : Lista de atributos agregados al esquema de Active Directory (continuación)

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Atributo: `dellAssociationMembers` **Descripción**: Lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso para el atributo vinculado dellProductMembers. **Identificación de vínculo**: 12071 **OID:** 1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellPermissionsMask1` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.1 número entero (LDAPTYPE_INTEGER)	
Atributo: `dellPermissionsMask2` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.2 número entero (LDAPTYPE_INTEGER)	

Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory

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

Cuando instala el software de administración de sistemas mediante el DVD *Dell Systems Management Tools and Documentation (Documentación y herramientas de Dell Systems Management)*, puede extender el complemento si selecciona la opción **Active Directory Users and Computers Snap-in (Complemento Usuarios y equipos de Active Directory)** durante el procedimiento de instalación. Consulte *Dell OpenManage Software Quick Installation Guide (Guía de instalación rápida del software Dell OpenManage)* para obtener instrucciones adicionales para la instalación del software de administración de sistemas. Para sistemas operativos Windows de 64 bits, el instalador del complemento se encuentra en `<unidaddeDVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64`

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

Agregar usuarios y privilegios del CMC a Active Directory

Mediante el complemento Usuarios y equipos de Active Directory extendido de Dell, puede agregar usuarios de la CMC y privilegios al crear objetos de dispositivo de RAC, de asociación y de privilegio. Para agregar cada objeto, haga lo siguiente:

- Cree un objeto de dispositivo de RAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Conceptos relacionados

Adición de objetos a un objeto de asociación en la página 148

Tareas relacionadas

Creación de un objeto de dispositivo de RAC en la página 147
Creación de un objeto de privilegio en la página 148
Creación de un objeto de asociación en la página 148

Creación de un objeto de dispositivo de RAC

Para crear un objeto de dispositivo de RAC:

1. En la ventana **Raíz de consola (MMC)**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** > **objeto Dell Remote Management**.

Se abre la ventana **Nuevo objeto**.

3. Introduzca un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre de la CMC que proporcionó en "Configuración de Active Directory con esquema extendido mediante la interfaz web de la CMC".
4. Seleccione **Objeto de dispositivo de RAC** y haga clic en **Aceptar**.

Creación de un objeto de privilegio

Para crear un objeto de privilegio:

NOTA: Debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola (MMC)**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.
   Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio** y haga clic en **Aceptar**.
5. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
6. Haga clic en la ficha **Privilegios de RAC** y asigne los privilegios para el usuario o grupo.
   Para obtener más información sobre los privilegios de usuario del CMC, consulte Tipos de usuarios.

Creación de un objeto de asociación

El objeto de asociación deriva de un grupo y debe contener un tipo de grupo. El ámbito de la asociación especifica el tipo de grupo de seguridad del objeto de asociación. Al crear un objeto de asociación, elija el ámbito de la asociación correspondiente al tipo de objeto que quiere agregar. Por ejemplo, si selecciona Universal los objetos de asociación solo estarán disponibles cuando el dominio de Active Directory funcione en el modo Native (Nativo) u otro superior.

Para crear un objeto de asociación:

1. En la ventana **Raíz de consola (MMC)**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo** > **Opciones avanzadas del objeto Dell Remote Management**.
   Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el nuevo objeto y seleccione **Objeto de asociación**.
4. Seleccione el ámbito para **Objeto de asociación** y haga clic en **Aceptar**.

Adición de objetos a un objeto de asociación

En la ventana **Association Object Properties (Propiedades de objeto de asociación)**, puede asociar usuarios o grupos de usuarios, objetos de privilegio, y dispositivos de RAC o grupos de dispositivos de RAC. Si el sistema se ejecuta en el modo de Microsoft Windows 2000 o superior, use grupos universales para expandir dominios con su usuario u objetos de RAC.

Es posible agregar grupos de usuarios y dispositivos de RAC. El procedimiento para crear grupos relacionados con Dell y grupos no relacionados con Dell es el mismo.

Tareas relacionadas

Adición de usuarios o grupos de usuarios en la página 148
Adición de privilegios en la página 149
Forma de agregar dispositivos de RAC o grupos de dispositivos de RAC en la página 149

Adición de usuarios o grupos de usuarios

Para agregar usuarios o grupos de usuarios:

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

Adición de privilegios

Para agregar privilegios:

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

   Haga clic en la ficha **Privilege Object (Objeto de privilegio)** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios al autentificar en un dispositivo de RAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

Forma de agregar dispositivos de RAC o grupos de dispositivos de RAC

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

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Introduzca el nombre de los dispositivos de RAC o de los grupos de dispositivos de RAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

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

Configuración de Active Directory con esquema extendido mediante la interfaz web del CMC

Para configurar Active Directory con esquema extendido mediante la interfaz web del CMC:

NOTA: Para obtener información acerca de los distintos campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Autentificación de usuario** > **Servicios de directorio**.
2. Seleccione **Microsoft Active Directory (esquema extendido)**.
   Las opciones a configurar para el esquema extendido aparecerán en la misma página.
3. Especifique lo siguiente:
   - Active Active Directory, proporcione el nombre de dominio raíz y el valor de tiempo de espera.
   - Si desea que la llamada dirigida realice una búsqueda en la controladora de dominio y el catálogo global, seleccione la opción **Buscar servidor de AD para la búsqueda (opcional)** y especifique los detalles de la controladora de dominio y el catálogo global.

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

     NOTA: Puede especificar una lista de servidores de controladora de dominio o de catálogo global separados por comas. La CMC le permite especificar hasta tres direcciones IP o nombres de host.

     NOTA: Los servidores de controladora de dominio y de catálogo global que no se han configurado correctamente para todos los dominios y las aplicaciones pueden producir resultados inesperados durante el funcionamiento de las aplicaciones o los dominios existentes.
4. Haga clic en **Aplicar** para guardar la configuración.

   NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.
5. En la sección **Configuración del esquema extendido**, escriba el nombre del dispositivo de CMC y el nombre de dominio.
6. Si ha activado la validación de certificados, debe cargar en el CMC el certificado firmado por una autoridad de certificados raíz para el bosque de dominio. En la sección **Administrar certificados**, escriba la ruta de acceso del archivo o busque el archivo de certificado. Haga clic en **Cargar** para cargar el archivo en el CMC.

   NOTA: El valor `File Path` muestra la ruta de acceso relativa del archivo de certificado que va a cargar. Debe escribir la ruta de acceso absoluta del archivo, que incluye la ruta de acceso completa más el nombre completo del archivo con la extensión.

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

PRECAUCIÓN: La validación del certificado SSL se requiere de forma predeterminada. Desactivar este certificado es peligroso.

7. Si ha activado el inicio de sesión único (SSO), en la sección Archivo keytab de Kerberos, haga clic en **Examinar**, especifique el archivo keytab y, a continuación, haga clic en **Cargar**.
   Al completarse la carga, aparecerá un mensaje que indica que la carga ha sido correcta o ha fallado.
8. Haga clic en **Aplicar**.
   El servidor web del CMC se reiniciará automáticamente.
9. Inicie sesión en la interfaz web del CMC.
10. En el árbol del sistema, seleccione **Chasis**, haga clic en la ficha **Red** y luego en la subficha **Red**.
    Aparecerá la página **Configuración de red**.
11. Si la opción **Usar DHCP** para la dirección IP de la interfaz de red del CMC está activada, siga uno de estos pasos:
    - Seleccione la opción **Usar DHCP para obtener direcciones de servidor DNS** para que el servidor DHCP obtenga automáticamente las direcciones del servidor DNS.
    - Configure manualmente la dirección IP de un servidor DNS sin seleccionar la opción **Use DHCP to Obtain DNS Server Addresses (Usar DHCP para obtener direcciones de servidor DNS)**. Escriba las direcciones IP del servidor DNS principal y alternativo en los campos provistos.
12. Haga clic en **Aplicar cambios**.
    Se habrán configurado las opciones de Active Directory para el esquema extendido.

Configuración de Active Directory con esquema extendido mediante RACADM

Para configurar Active Directory en el CMC con esquema extendido mediante RACADM:

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o
cfgADRacDomain <fully qualified CMC domain name>
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <fully qualified root domain name>
racadm config -g cfgActiveDirectory -o
cfgADRacName <CMC common name>
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate> -r
racadm sslcertdownload -t 0x1 -f <CMC SSL certificate>
```

NOTA: Este comando se puede usar solamente a través de RACADM remoto. Para obtener más información acerca de RACADM remoto, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

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

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

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

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

Para especificar un servidor de LDAP, escriba:

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController <AD domain controller IP address>
```

Para especificar un servidor de catálogo global, escriba:

```
racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog <AD global catalog IP address>
```

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

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

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

2. Especifique un servidor DNS por medio de una de las siguientes opciones:
   - Si DHCP está activado en el CMC y desea utilizar la dirección de DNS obtenida automáticamente mediante el servidor DHCP, escriba el siguiente comando:

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

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

     ```
     racadm config -g cfgLanNetworking -o
     cfgDNSServersFromDHCP 0
     racadm config -g cfgLanNetworking -o
     cfgDNSServer1 <primary DNS IP address>
     racadm config -g cfgLanNetworking -o
     cfgDNSServer2 <secondary DNS IP address>
     ```

De esta forma, se completa la configuración de la función de esquema extendido.

Configuración de los usuarios LDAP genéricos

La CMC ofrece una solución genérica para admitir la autentificación basada en el protocolo ligero de acceso a directorios (LDAP). Esta función no requiere ninguna extensión del esquema en los servicios de directorio.

Ahora un administrador de la CMC puede integrar los inicios de sesión de los usuarios del servidor LDAP con la CMC. Esta integración requiere una configuración en el servidor LDAP y en la CMC. En el servidor LDAP, se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso a la CMC se convierte en miembro del grupo de funciones. Los privilegios se continúan almacenando en la CMC para la autorización de forma similar a la configuración de esquema estándar compatible con Active Directory.

Para habilitar el acceso del usuario de LDAP 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. Existe la opción de agregar un usuario a varios grupos dentro del servicio de directorio. Si un usuario es miembro de varios grupos, obtiene los privilegios de todos sus grupos.

Para obtener información sobre el nivel de privilegios de los grupos de funciones y los valores predeterminados de esos grupos, consulte Tipos de usuarios.

En la siguiente figura se ilustra la configuración del CMC con el servicio LDAP genérico.

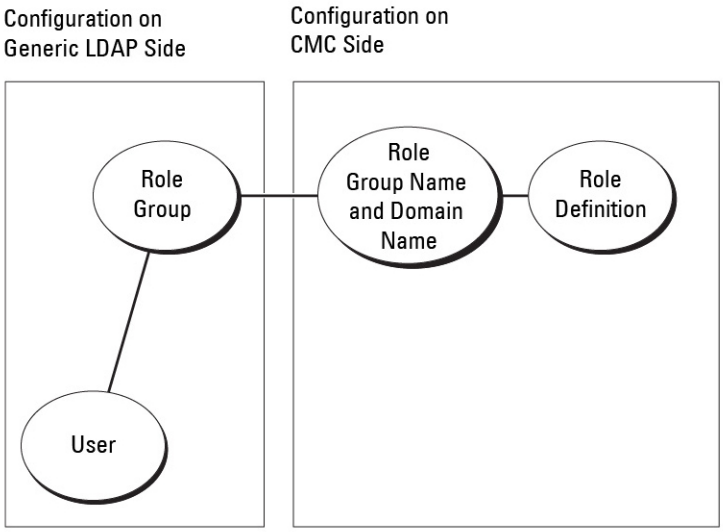


Ilustración 11. Configuración de CMC con LDAP genérico

Configuración del directorio LDAP genérico para acceder a CMC

La implementación de LDAP genérico del CMC utiliza dos fases para otorgar acceso a la autentificación usuario-usuario y a la autorización de usuarios.

Autentificación de usuarios LDAP

Algunos servidores de directorios requieren un enlace para poder realizar búsquedas en un servidor LDAP específico.

Para autentificar un usuario:

1. Establezca un enlace opcional con el servicio de directorio. La opción predeterminada es un enlace anónimo.

   NOTA: Los servidores de directorios basados en Windows no permiten inicio de sesión anónimo. Por lo tanto, introduzca el nombre de dominio y la contraseña del enlace.

2. Busque al usuario por su nombre de usuario. El atributo predeterminado es `uid`.
   Si se encuentra más de un objeto, el proceso arroja un mensaje de error.
3. Anule el enlace y establezca un enlace con el DN y la contraseña de usuario.
   Si el enlace falla, fallará el inicio de sesión.

Si estos pasos se completan correctamente, el usuario se considera autentificado.

Autorización de usuarios LDAP

Para autorizar un usuario:

1. Busque en cada grupo configurado el nombre de dominio del usuario dentro de los atributos `member or uniqueMember`.
2. Para cada grupo al que pertenezca el usuario, se agregarán en forma conjunta los privilegios de todos los grupos.

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web del CMC

Para configurar el servicio de directorio LDAP genérico:

NOTA: Es necesario contar con el privilegio de **Administrador de configuración del chasis**.

1. En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **User Authentication (Autentificación de usuario)** > **Directory Services (Servicios de directorio)**.

2. Seleccione **LDAP** genérico.
   Los valores que se deben configurar para el esquema estándar se mostrarán en la misma página.
3. Especifique lo siguiente:

   NOTA: Para obtener información acerca de los distintos campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

   - 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*> es el nombre del servicio para utilizar en la consulta.

       Por ejemplo:

       ```
       _ldap._tcp.dell.com
       ```

       donde `ldap` es el nombre del servicio y `dell.com` es el dominio de la 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**. Aparecerá la página **Configure LDAP Role Group (Configurar grupo de funciones de LDAP)**.
6. Especifique el nombre de dominio del grupo y los privilegios 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 de los grupos RACADM `cfgLdap` y `cfgLdapRoleGroup`.

Existen muchas opciones para configurar los inicios de sesión de LDAP. En la mayoría de los casos, algunas opciones pueden utilizarse con su configuración predeterminada.

NOTA: Se recomienda encarecidamente que utilice el comando racadm `testfeature -f LDAP` para probar la configuración inicial de LDAP. Esta función admite IPv4 e IPv6.

Los cambios de propiedades necesarios incluyen la activación de inicios de sesión de LDAP, la definición de un nombre de dominio completo o una dirección IP para el servidor y la configuración del DN de base del servidor LDAP.

- ```
  $ racadm config -g cfgLDAP -o cfgLDAPEnable 1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=
  company,dc=com
  ```
  ```

La CMC puede configurarse para solicitar de forma opcional registros de SRV al servidor DNS. Si la propiedad `cfgLDAPSRVLookupEnable` está activada, no se hace caso a la propiedad `cfgLDAPServer`. La siguiente consulta se utiliza para buscar registros de SRV en el DNS:

```
_ldap._tcp.domainname.com
```

`ldap` en la consulta anterior es la propiedad `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` se configura para que sea **domainname.com**.

Para obtener más información acerca de los objetos RACADM, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) disponible en **dell.com/support/manuals**.

10

Configuración del CMC para inicio de sesión único o inicio de sesión mediante tarjeta inteligente

En esta sección se proporciona información para configurar la CMC para el inicio de sesión único (SSO) y el inicio de sesión mediante tarjeta inteligente en los usuarios de Active Directory.

A partir de la versión 2.10, el CMC admite la autentificación de Active Directory basada en Kerberos para el inicio de sesión único y el inicio de sesión mediante tarjeta inteligente.

El inicio de sesión único utiliza Kerberos como método de autentificación, lo que permite que los usuarios que han iniciado sesión en el dominio cuenten con un inicio de sesión único o automático en las aplicaciones subsiguientes como Exchange. Para el inicio de sesión único, la CMC utiliza las credenciales del sistema cliente, las cuales el sistema operativo almacena en caché después de que el usuario inicia sesión mediante una cuenta válida de Active Directory.

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, como SSH. En las demás interfaces de inicio de sesión también hay que definir los atributos de política. Si desea desactivar todas las demás interfaces de inicio de sesión, vaya a la página **Services (Servicios)** y desactive las interfaces que desee.

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.

Conceptos relacionados

Requisitos del sistema en la página 155
Prerrequisitos para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente en la página 156
Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory en la página 158

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 Windows 2003, asegúrese de tener las revisiones y los Service Pack más recientes instalados en el sistema cliente. Si usa Active Directory en 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=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- Para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente, el sistema cliente debe formar parte del dominio de Active Directory y del territorio de Kerberos.

CMC

- El CMC debe tener la versión de firmware 2.10 o superior.
- Cada CMC debe tener una cuenta de Active Directory.
- El CMC debe formar parte del dominio de Active Directory y del territorio de Kerberos.

Prerrequisitos para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente

A continuación se indican los prerrequisitos para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente:

- Configure el territorio de Kerberos y el centro de distribución de claves (KDC) para Active Directory (ksetup).
- Una sólida infraestructura de NTP y DNS para evitar problemas de desfase de tiempo y búsqueda inversa.
- Configure la CMC y el grupo de funciones de esquema estándar de Active Directory con miembros autorizados.
- Para la tarjeta inteligente, cree usuarios de Active Directory para cada CMC, configurados para utilizar el cifrado DES de Kerberos pero no la preautentificación.
- Configure el explorador para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente.
- Registre a los usuarios de CMC en el centro de distribución de claves con Ktpass (esto también genera una clave que se carga en la CMC).

Conceptos relacionados

Configuración del esquema estándar de Active Directory en la página 139
Configuración del esquema extendido de Active Directory en la página 143
Configuración del explorador para el inicio de sesión único en la página 157

Tareas relacionadas

Generación del archivo Keytab de Kerberos en la página 156
Configuración de un explorador para el inicio de sesión mediante tarjeta inteligente en la página 157

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 (ofrecida por Microsoft en el CD/DVD de instalación de servidores) se utiliza para crear los enlaces entre el nombre principal de servicio (SPN) y una cuenta de usuario, y para exportar la información de confianza a un archivo keytab de Kerberos de estilo MIT. Para obtener más información sobre la utilidad ktpass, consulte el sitio web de Microsoft.

Antes de generar un archivo keytab, debe crear una cuenta de usuario de Active Directory para usar con la opción **-mapuser** del comando ktpass. El nombre utilizado debe ser igual al del DNS de la CMC donde cargue 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.domainname.com@DOMAINNAME.COM -mapuser keytabuser -crypto
DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

NOTA: Debe introducir `cmcname.domainname.com` en minúsculas, como exige RFC, mientras que `@REALM_NAME` debe estar en mayúsculas. Además, la CMC admite el tipo de criptografía DES-CBC-MD5 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 del CMC para el esquema de Active Directory

Para obtener información sobre la forma de configurar el CMC para el esquema estándar de Active Directory, consulte Configuring Standard Schema Active Directory (Configuración del esquema estándar de Active Directory).

Para obtener información sobre la forma de configurar el CMC para el esquema extendido de Active Directory, consulte Extended Schema Active Directory Overview (Descripción general del esquema extendido de Active Directory).

Configuración del explorador para el inicio de sesión único

El inicio de sesión único (SSO) es compatible con Internet Explorer versiones 6.0 y superiores, y Firefox versiones 3.0 y superiores.

NOTA: Las instrucciones siguientes se aplican solamente si la CMC utiliza el inicio de sesión único con la autentificación de Kerberos.

Internet Explorer

Para configurar Internet Explorer para inicio de sesión único:

1. En Internet Explorer, seleccione **Herramientas** > **Opciones de Internet**.
2. En la ficha **Seguridad**, en **Seleccione una zona para ver o cambiar la configuración de seguridad**, seleccione **Intranet local**.
3. Haga clic en **Sitios**.
   Se muestra el cuadro de diálogo **Intranet local**.
4. Haga clic en **Advanced (Opciones avanzadas)**.
   Se muestra el cuadro de diálogo **Configuración avanzada de Intranet local**.
5. En el campo **Agregar este sitio a la zona**, escriba el nombre del CMC y el dominio al cual pertenece y haga clic en **Agregar**.

   NOTA: Se puede utilizar un comodín (*) para especificar todos los dispositivos o usuarios de ese dominio.

Mozilla Firefox

1. En Firefox, escriba `about:config` en la barra de direcciones.

   NOTA: Si el navegador muestra la advertencia **This might void your warranty (Esto puede anular su garantía)**, haga clic en **I'll be careful (Seré cuidadoso)**. **I promise (Lo prometo)**.
2. En el cuadro de texto **Filtro**, escriba `negotiate`.
   El explorador muestra una lista de nombres preferidos limitada a aquéllos que contienen la palabra "negotiate".
3. En la lista, haga doble clic en **network.negotiate-auth.trusted-uris**.
4. En el cuadro de diálogo **Ingresar valor de la cadena**, escriba el nombre de dominio del CMC y haga clic en **Aceptar**.

Configuración de un explorador para el inicio de sesión mediante tarjeta inteligente

Mozilla Firefox: el CMC 2.10 no admite el inicio de sesión mediante tarjeta inteligente a través del explorador Firefox.

Internet Explorer: asegúrese de que el explorador de Internet esté configurado para descargar los complementos Active-X.

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory

Es posible usar la interfaz web del CMC o RACADM para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente en el CMC.

Tareas relacionadas

Prerrequisitos para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente en la página 156
Cómo cargar el archivo keytab en la página 158

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory mediante la interfaz web

Para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente de Active Directory en el CMC:

NOTA: Para obtener más información acerca de estas opciones, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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: Todas las interfaces fuera de banda de línea de comandos, incluidas Secure Shell (SSH), Telnet, serie y RACADM remoto, se mantienen sin cambios cuando se selecciona esta opción.
2. Haga clic en **Aplicar**.

   La configuración se guarda.

   Es posible probar Active Directory con la autentificación de Kerberos mediante el comando de RACADM:

   ```
   testfeature -f adkrb -u <user>@<domain>
   ```

   donde `<user>` es una cuenta de usuario de Active Directory válida.

   Una ejecución satisfactoria de este comando indica que la CMC puede adquirir credenciales Kerberos y acceder a la cuenta de Active Directory del usuario. Si el comando no se ejecuta satisfactoriamente, resuelva el error y vuelva a ejecutar el comando. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)* en **dell.com/support/manuals**.

Cómo cargar el 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 territorio de Kerberos se debe registrar con Active Directory y debe tener un archivo keytab exclusivo.

Usted puede cargar un archivo keytab de Kerberos generado en el servidor de Active Directory asociado. Se puede generar el archivo keytab de Kerberos desde el servidor de Active Directory ejecutando la utilidad `ktpass.exe`. Este archivo keytab establece una relación de confianza entre el servidor de Active Directory Server y la CMC.

Para cargar el archivo keytab:

1. En el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **User Authentication (Autentificación de usuario)** > **Directory Services (Servicios de directorio)**.
2. Seleccione **Microsoft Active Directory (Esquema estándar)**.
3. En la sección **Archivo keytab de Kerberos**, haga clic en **Examinar**, seleccione el archivo keytab y haga clic en **Cargar**.

   Una vez completada la carga, se mostrará un mensaje donde se indicará si el archivo keytab se ha cargado correctamente o no.

Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory mediante RACADM

Además de los pasos que se realizan durante la configuración de Active Directory, ejecute el siguiente comando para activar el inicio de sesión único:

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

Además de los pasos que se realizan durante la configuración de Active Directory, utilice los siguientes objetos para activar el inicio de sesión mediante tarjeta inteligente:

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

Configuración del CMC para el uso de consolas de línea de comandos

En esta sección se proporciona información acerca de las funciones de la consola de línea de comandos (o la consola de serie/Telnet/Secure Shell) de la CMC y se indica cómo configurar el sistema para poder ejecutar acciones de administración de sistemas a través de la consola. Para obtener más información sobre el uso de los comandos RACADM en la CMC a través de la consola de línea de comandos, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Tareas relacionadas

Antes de iniciar sesión en el CMC mediante una consola serie, Telnet o SSH en la página 41

Temas:

Funciones de la consola de línea de comandos del CMC

La CMC admite las siguientes funciones de consola serie, Telnet y SSH:

- Una conexión de cliente serie y hasta cuatro conexiones simultáneas de cliente Telnet.
- Hasta cuatro conexiones simultáneas de cliente Secure Shell (SSH).
- Compatibilidad para comandos RACADM.
- Comando connect integrado que conecta a la consola serie de servidores y 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 línea de comandos del CMC

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

Tabla 31. : Comandos para la línea de comandos del CMC

Comando	Descripción
`racadm`	Los comandos RACADM comienzan con la palabra clave `racadm` y siguen con un subcomando. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.
`connect`	Conecta a la consola serie de un servidor o módulo de E/S. Para obtener más información, consulte Conexión a servidores o módulos de E/S con el comando connect. **NOTA:** También puede usar el comando racadm `connect`.

Tabla 31. : Comandos para la línea de comandos del CMC (continuación)

Comando	Descripción
`exit`, `logout` y `quit`	Todos los comandos ejecutan la misma acción. Terminan la sesión actual y regresan a una pantalla de inicio de sesión.

Uso de una consola Telnet con el CMC

Es posible mantener hasta cuatro sesiones Telnet con la CMC de forma simultánea.

Si la estación de administración ejecuta Microsoft Windows XP o Windows 2003, es posible que tenga un problema con los caracteres en las sesiones Telnet de la CMC. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión por el cual la tecla Intro no responde y no aparece la petición de contraseña.

Para solucionar este problema, descargue la corrección urgente 824810 en **support.microsoft.com**. Además, puede consultar el artículo 824810 de la Base de conocimientos de Microsoft para obtener más información.

En la interfaz de la línea de comandos, puede administrar los tiempos de espera de las sesiones a través del comando racadm, `racadm getconfig -g cfgSessionManagement`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

Uso de SSH con el CMC

SSH es una sesión de línea de comandos que incluye las mismas funciones que una sesión Telnet, pero con cifrado y negociación de sesiones para mejorar la seguridad. La CMC admite la versión 2 de SSH con autentificación de contraseñas. SSH viene activada en la CMC de forma 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 emite un mensaje de error. El texto del mensaje depende del cliente y no es controlado por la CMC. Lea 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` en el símbolo del sistema de Windows, no se obtienen todas las funciones (es decir, algunas teclas no responden y no se muestran gráficos). En sistemas con Linux, ejecute los servicios cliente de SSH para conectarse a la CMC con cualquier shell.

Se admiten cuatro sesiones simultáneas de SSH. El tiempo de espera de la sesión es controlado por la propiedad `cfgSsnMgtSshIdleTimeout`. Para obtener más información, consulte el capítulo sobre propiedades de la base de datos de *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*, la página **Services Management (Administración de servicios)** en la interfaz web, o bien Configuración de servicios.

La CMC también admite autentificación de clave pública (PKA) en SSH. Este método de autentificación mejora la automatización de las secuencias de comandos de SSH, al evitar la necesidad de incorporar o solicitar la Id. de usuario/contraseña. Para obtener más información, consulte Configuración de la autentificación de clave pública en SSH.

SSH viene activada de forma predeterminada. Cuando está desactivada, es posible activarla por medio de cualquier otra interfaz admitida.

Para configurar SSH, consulte Configuring Services (Configuración de servicios).

Conceptos relacionados

Configuración de servicios en la página 83

Esquemas de criptografía SSH compatibles

Para comunicarse con la CMC mediante el protocolo SSH, se admiten varios esquemas de criptografía que se enumeran en la tabla siguiente.

Tabla 32. Esquemas de criptografía

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

Configuración de la autentificación de clave pública en SSH

Puede configurar hasta 6 claves públicas que se pueden utilizar con el nombre de usuario service en la interfaz de SSH. Antes de agregar o eliminar claves públicas, asegúrese de utilizar el comando view para ver las claves que ya están configuradas y no sobrescribir ni eliminar accidentalmente ninguna. El nombre de usuario service es una cuenta de usuario especial que se puede utilizar al acceder a la CMC mediante SSH. Cuando la autentificación de clave pública en SSH se configura y se utiliza correctamente, no es necesario introducir un nombre de usuario ni una contraseña para iniciar sesión en la CMC. Esta función puede resultar de gran utilidad para configurar secuencias de comandos automáticas para ejecutar diversas funciones.

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

Al agregar claves públicas nuevas, asegúrese de que las claves existentes no se encuentren ya en el índice donde desea agregar la clave nueva. La CMC no realiza controles para verificar que las claves anteriores se hayan eliminado antes de agregar una nueva. Tan pronto como se agrega una clave nueva, esa clave entra en vigor automáticamente, siempre y cuando la interfaz de SSH esté activada.

Cuando utilice la sección de comentario de la clave pública, recuerde que la CMC solo utiliza los primeros 16 caracteres. La CMC utiliza el comentario de la clave pública para distinguir a los usuarios de SSH cuando se utiliza el comando RACADM `getssninfo`, ya que todos los usuarios de autentificación de clave pública usan el nombre de usuario service para iniciar sesión.

Por ejemplo, si se configuran dos claves públicas, una con el comentario PC1 y otra con el PC2:

```
racadm getssninfo
Type       User   IP Address   Login
Date/Time
SSH        PC1    x.x.x.x      06/16/2009
09:00:00
SSH        PC2    x.x.x.x      06/16/2009
09:00:00
```

Para obtener más información sobre `sshpkauth`, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Tareas relacionadas

Generación de claves públicas para sistemas que ejecutan Windows en la página 163
Generación de claves públicas para sistemas que ejecutan Linux en la página 163
Notas de la sintaxis de RACADM para CMC en la página 163
Visualización de claves públicas en la página 163
Adición de claves públicas en la página 164

Eliminación de claves públicas en la página 164

Generación de claves públicas para sistemas que ejecutan Windows

Antes de agregar una cuenta, se requiere una clave pública del sistema que accede a la CMC en SSH. Hay dos maneras de generar el par de claves pública/privada: mediante la aplicación PuTTY Key Generator (Generador de claves PuTTY) para clientes con Windows, o mediante la CLI ssh-keygen para clientes con Linux.

En esta sección se presentan instrucciones sencillas para generar un par de claves pública/privada para ambas aplicaciones. Para ver usos adicionales o avanzados de estas herramientas, consulte la ayuda de la aplicación.

Si desea usar el generador de claves PuTTY para crear la clave básica para sistemas que ejecutan clientes Windows:

1. Inicie la aplicación y seleccione SSH-2 RSA para el tipo de clave que generará (SSH-1 no es compatible).
2. Especifique la cantidad de bits de la clave. El tamaño de la clave RSA debería estar entre 2048 y 4096.

   NOTA:
   - Es posible que la CMC no muestre un mensaje si se agregan claves menores de 2048 o mayores de 4096, pero estas claves fallan al intentar iniciar sesión.
   - La CMC acepta las claves RSA hasta la fortaleza de clave 4096, pero la fortaleza de clave recomendada es 2048.

3. Haga clic en **Generar** y mueva el mouse dentro de la ventana como se indica.

   Después de crear la clave, se puede modificar el campo de comentario de la clave.

   También puede introducir 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 símbolo shell del sistema, escriba:

```
ssh-keygen -t rsa -b 2048 -C testing
```

donde:

`-t` debe ser rsa.

`-b` especifica el tamaño de cifrado de bits entre 2048 y 4096.

`-c` permite modificar el comentario de clave pública y es opcional.

`<passphrase>` es opcional. Después de completar el comando, utilice el archivo público para pasar a RACADM y cargar el archivo.

Notas de la sintaxis de RACADM para CMC

Cuando utilice el comando `racadm sshpkauth`, asegúrese de lo siguiente:

- Para la opción `-i` , el parámetro debe ser `svcacct`. Todos los demás parámetros para `-i` fallan en la CMC. `svcacct` es una cuenta especial para la autentificación de claves públicas por SSH en la CMC.
- Para iniciar sesión en la CMC, el usuario debe ser service. Los usuarios de otras categorías tienen acceso a las claves públicas introducidas mediante el comando `sshpkauth`.

Visualización de claves públicas

Para ver las claves públicas que se han agregado al CMC, escriba:

```
racadm sshpkauth -i svcacct -k all -v
```

Para ver una clave a la vez, reemplace `all` con un número del 1 al 6. Por ejemplo, para ver la clave 2, escriba:

```
racadm sshpkauth -i svcacct -k 2 -v
```

Adición de claves públicas

Para agregar una clave pública a la CMC mediante la opción de carga de archivo `-f`, escriba:

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -f <public key file>
```

NOTA: Solo puede usar la opción de carga de archivo con RACADM remoto. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Para agregar una clave pública mediante la opción de carga de texto, escriba:

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -t "<public key text>"
```

Eliminación de claves públicas

Para eliminar una clave pública, escriba:

```
racadm sshpkauth -i svcacct -k 1 -d
```

Para eliminar todas las claves públicas, escriba:

```
racadm sshpkauth -i svcacct -k all -d
```

Activación del panel frontal para la conexión del iKVM

Para obtener información e instrucciones sobre el uso de los puertos del panel frontal del iKVM, consulte Enabling or Disabling Access to iKVM from Front Panel (Activación o desactivación del acceso al iKVM desde el panel frontal).

Configuración del software de emulación de terminal

El CMC admite una consola de texto en serie de una estación de administración si ejecuta uno de los siguientes tipos de software de emulación de terminal:

- Minicom de Linux.
- HyperTerminal Private Edition (versión 6.3) de Hilgraeve.

Lleve a cabo los pasos en los apartados siguientes para configurar el tipo de software de terminal necesario.

Configuración de Minicom de Linux

Minicom es una utilidad de acceso a puertos serie para Linux. Los pasos siguientes son válidos para configurar Minicom versión 2.0. Otras versiones de Minicom pueden diferenciarse ligeramente, pero requieren la misma configuración básica. Consulte la información de la sección Configuración necesaria para Minicom para configurar otras versiones de Minicom.

Configuración de Minicom versión 2.0

NOTA: Para obtener los mejores resultados, configure la propiedad **cfgSerialConsoleColumns** de manera que coincida con el número de columnas. Tenga en cuenta que el símbolo del sistema ocupa dos caracteres. Por ejemplo, para una ventana de terminal con 80 columnas:

```
racadm config -g cfgSerial -o
cfgSerialConsoleColumns 80.
```

1. Si no tiene el archivo de configuración de Minicom, avance al siguiente paso. Si tiene un archivo de configuración de Minicom, escriba `minicom<Minicom config file name>` y avance al paso 12.
2. En el símbolo del sistema de Linux, escriba `minicom -s`.
3. Seleccione **Configuración del puerto serie** y presione <Intro>.
4. Presione <a> y seleccione el dispositivo serie correspondiente (por ejemplo, `/dev/ttyS0`).
5. Presione <e> y defina la opción **Bps/Par/Bits** con el valor **115200 8N1**.
6. Presione <f>, y luego configure **Hardware Flow Control** (**Control de flujo de hardware)** en **Yes (Sí)** y **Software Flow Control** (**Control de flujo de software)** en **No**. Para salir del menú **Serial Port Setup (Configuración de puerto serie)**, pulse <Intro>.
7. Seleccione **Módem y marcación** y presione <Intro>.
8. En el menú **Configuración de parámetros y marcación de módem**, presione <Retroceso> para borrar los valores **init**, **reset**, **connect** y **hangup** de modo que queden en blanco; luego presione <Intro> para guardar cada valor en blanco.
9. Cuando se hayan borrado todos los campos especificados, presione <Intro> para salir del menú **Configuración de parámetros y marcación de módem**.
10. Seleccione **Salir de Minicom** y presione <Intro>.
11. En el símbolo shell del sistema, escriba `minicom <Minicom config file name>`.
12. Presione <Ctrl><a>, <x> o <Intro> para salir de Minicom.

    Asegúrese de que la ventana **Minicom** muestre una petición de inicio de sesión. Cuando aparezca, la conexión se habrá completado con éxito. Desde ese momento, podrá iniciar sesión y acceder a la interfaz de línea de comandos de la CMC.

Valores de Minicom necesarios

Consulte la siguiente tabla para configurar cualquier versión de Minicom.

Tabla 33. Configuración de Minicom

Descripción del valor	Valor necesario
Bps/Par/Bits	115200 8N1
Control de flujo de hardware	Sí
Control de flujo de software	No
Emulación de terminal	ANSI
Configuración de parámetros y marcación de módem	Borre los valores **init**, **reset**, **connect** y **hangup** de modo que queden en blanco.

Conexión a servidores o módulos de entrada y salida con el comando connect

El 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:

- el comando `racadm connect`. Para obtener más información, consulte Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e) en **dell.com/support/manuals**.
- La función de redirección de consola serie de la interfaz web del iDRAC.

- La función de comunicación en serie en la LAN (SOL) del iDRAC.

En una consola serie/Telnet/SSH, la CMC admite el comando connect para establecer una conexión serie con un servidor o módulos de E/S. La consola serie del servidor contiene las pantallas de inicio y configuración del BIOS, y también la consola serie del sistema operativo. Para los módulos de E/S, está disponible la consola serie del conmutador.

PRECAUCIÓN: Cuando se ejecuta desde la consola serie de la CMC, la opción `connect -b` permanece conectada hasta que se restablece la CMC. Esta conexión constituye un potencial riesgo de seguridad.

NOTA: El comando `connect` proporciona la opción `–b` (binaria). La opción `–b` transmite datos binarios sin procesar, y no se utiliza `cfgSerialConsoleQuitKey`. Además, al conectarse a un servidor por medio de la consola serie de la CMC, las transiciones en la señal DTR (por ejemplo, si se quita el cable serie para conectar un depurador) no causan una desconexión.

NOTA: Si un módulo de E/S no admite redirección de consola, el comando `connect` muestra una consola vacía. En tal caso, para regresar a la consola de la CMC, escriba la secuencia de escape. La secuencia de escape de consola predeterminada es <CTRL><\>.

Existen hasta seis módulos de E/S en el sistema administrado. Para conectarse a un módulo de E/S escriba:

```
connect switch-n
```

donde `n` es una etiqueta del módulo de E/S A1, A2, B1, B2, C1 y C2.

(Consulte la Figura 13-1 para ver una ilustración de la colocación de los módulos de E/S en el chasis). Cuando se hace referencia a los módulos de E/S en el comando connect, los módulos de E/S se asignan a conmutadores como se muestra en la tabla siguiente.

Tabla 34. : Asignación de módulos de E/S a conmutadores

Etiqueta del módulo de E/S	Conmutador
A1	switch-a1 o switch- 1
A2	switch-a2 o switch- 2
B1	switch-b1 o switch-3
B2	switch-b2 o switch-4
C1	switch-c1 o switch-5
C2	switch-c2 o switch-6

NOTA: Solo puede haber una conexión de módulo de E/S por chasis al mismo tiempo.

NOTA: No es posible establecer conexiones de paso desde la consola serie.

Para conectarse a una consola serie de servidor administrado, utilice el comando `connect server-<n><x>`, donde *n* es 1-8 y *x* es a, b, c o d. También puede usar el comando `racadm connect server-n`. Cuando se conecta a un servidor por medio de la opción `–b`, se da por sentada la existencia de una comunicación binaria y se desactiva el carácter de escape. Si la iDRAC no se encuentra disponible, aparecerá el mensaje de error `No route to host`.

El comando `connect server-n` permite al usuario acceder al puerto serie del servidor. Tras establecerse la conexión, el usuario podrá ver la redirección de consola del servidor a través del puerto serie de la CMC que incluye la consola serie del BIOS y la consola serie del sistema operativo.

NOTA: Para ver las pantallas de inicio del BIOS, es necesario activar la redirección serie en la configuración del BIOS de los servidores. Además, la ventana del emulador de terminal se debe configurar en 80 x 25. De lo contrario, la pantalla resulta ilegible.

NOTA: No todas las teclas funcionan en las pantallas de configuración del BIOS, de manera que es necesario proporcionar secuencias de escape adecuadas para **CTRL+ALT+SUPR** y otras secuencias de escape. La pantalla de redirección inicial muestra las secuencias de escape necesarias.

Tareas relacionadas

Configuración del BIOS del servidor administrado para la redirección de consola serie en la página 167
Configuración de Windows para la redirección de consola en serie en la página 167
Configuración de Linux para la redirección de la consola en serie del servidor durante el inicio en la página 167
Configuración de Linux para la redirección de consola serie del servidor después del inicio en la página 168

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

Es necesario conectarse al servidor administrado por medio del iKVM (consulte Administración de servidores con iKVM o establecer una sesión de la consola remota desde la interfaz web del iDRAC (consulte *iDRAC User's Guide* (Guía del usuario del iDRAC) en **dell.com/support/manuals**).

La comunicación serie del BIOS está desactivada de forma predeterminada. Para redirigir los datos de la consola de texto del host a la comunicación en serie en la LAN, debe activar la redirección de consola a través de COM1. Para cambiar la configuración del BIOS:

1. Inicie el servidor administrado.
2. Presione <F2> para acceder a la utilidad de configuración del BIOS durante la autoprueba de encendido.
3. Desplácese hacia abajo hasta **Serial Communication (Comunicación serie)** y pulse <Intro>. En el cuadro de diálogo emergente, la lista de comunicación serie muestra las siguientes opciones:
   - Apagado
   - Encendido sin redirección de consola
   - Encendido con redirección de consola a través de COM1

   Utilice las teclas de flecha para recorrer las opciones.
4. Asegúrese de que la opción **Encendido con redirección de consola a través de COM1** esté activada.
5. Active **Redirection After Boot (Redirección después de inicio)**; el valor predeterminado es **Disabled (Desactivada)**. Esta opción permite la redirección de consola del BIOS en inicios posteriores.
6. Permite guardar los cambios y salir.

   El servidor administrado se reinicia.

Configuración de Windows para la redirección de consola en serie

No es necesario configurar los servidores que ejecutan Microsoft Windows Server a partir de la versión 2003. Windows recibirá información del BIOS y activará la consola de administración especial (SAC) en COM1.

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

Los pasos siguientes corresponden solo a Linux GRand Unified Bootloader (GRUB). Se deben realizar cambios similares si se utiliza un cargador de inicio diferente.

NOTA: Cuando configure la ventana de emulación de cliente VT100, establezca la ventana o aplicación que esté mostrando la consola redirigida en 25 filas x 80 columnas a fin de garantizar que el texto se muestre correctamente; de lo contrario, es posible que algunas pantallas de texto aparezcan ilegibles.

Modifique el archivo `/etc/grub.conf` 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 `/etc/grub.conf` contiene una directiva `splashimage`, inserte un carácter de comentario al inicio de la línea para anularla.

   El siguiente ejemplo ilustra los cambios descritos en este procedimiento.

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

```
# to this file
# NOTICE: You do not have a /boot partition. This
means that
# all kernel and initrd paths are relative to
/, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=
/dev/sdal
# initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial
title Red Hat Linux Advanced Server (2.4.9-e.3smp)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=
/dev/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 de texto. De lo contrario, la pantalla de GRUB no se mostrará en la redirección de la consola. Para desactivar la interfaz gráfica, inserte un carácter de comentario al inicio de la línea que empieza 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 que se agregó `console=ttyS1,57600` solo en la primera opción.

Configuración de Linux para la redirección de consola serie del servidor después del inicio

Modifique 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
```

Modifique el archivo `/etc/securetty`, como se indica a continuación:

Agregue una nueva línea, con el nombre del tty serie para COM2:

```
ttyS1
```

El siguiente ejemplo muestra un archivo con la nueva línea.

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
```

```
tty11
ttyS1
```

12

Uso de las tarjetas FlexAddress y FlexAddress Plus

Esta sección proporciona información acerca de la configuración y del uso de las tarjetas FlexAddress y FlexAddress Plus.

Conceptos relacionados

Acerca de FlexAddress en la página 171
Acerca de FlexAddress Plus en la página 172
Comparación entre FlexAddress y FlexAddress Plus en la página 172

Temas:

Acerca de FlexAddress

Si se reemplaza un servidor, la función FlexAddress de la ranura sigue siendo igual para la ranura del servidor dado. Si el servidor se inserta en una nueva ranura o un nuevo chasis, se utiliza la WWN/MAC asignada por el servidor, a menos que el chasis tenga la función FlexAddress activada para la ranura nueva. Si quita el servidor, regresará a la dirección asignada por el servidor. No es necesario volver a configurar los marcos de implementación, los servidores DHCP y los enrutadores de diversas redes Fabric para identificar el servidor nuevo.

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

FlexAddress permite que la CMC asigne Id. de WWN/MAC a una ranura determinada y anule las Id. de fábrica. Por ende, si se sustituye el módulo de servidor, las Id. de WWN/MAC basadas en la ranura no cambian. Gracias a esta función, ya no es necesario volver a configurar las herramientas de administración de redes Ethernet y los recursos SAN para un nuevo módulo de servidor.

Además, la anulación solo se produce cuando se inserta un módulo de servidor en un chasis con FlexAddress activado; no se realizan cambios definitivos 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.

La tarjeta de función FlexAddress contiene un rango de direcciones MAC. Antes de instalar FlexAddress, para determinar el rango de direcciones MAC de en una tarjeta de función FlexAddress, puede insertar la tarjeta SD en un lector de tarjetas de memoria USB y consultar el archivo `pwwn_mac.xml`. Este archivo XML de texto no cifrado de la tarjeta SD contiene una etiqueta XML *mac_start* que es la primera dirección MAC hexadecimal inicial utilizada para este rango exclusivo de direcciones MAC. La etiqueta *mac_count* es el

número total de direcciones MAC que asigna la tarjeta SD. El rango total de direcciones MAC asignadas se puede determinar de la manera siguiente:

```
<mac_start> + 0xCF (208 - 1) = mac_end
```

donde 208 es *mac_count* y la fórmula es:

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

Por ejemplo:

```
(starting_mac)00188BFFDCFA + (mac_count)0xCF - 1 = (ending_mac)00188BFFDDC8
```

NOTA: Bloquee la tarjeta SD antes de insertarla en el lector de tarjetas de memoria USB para no modificar accidentalmente el contenido. *Debe desbloquear* la tarjeta SD antes de insertarla en la CMC.

Acerca de FlexAddress Plus

FlexAddress Plus es una nueva función que se agrega en la versión 2.0 de la tarjeta de función. Se trata de una actualización de la tarjeta de función FlexAddress versión 1.0. FlexAddress Plus contiene más direcciones MAC que FlexAddress. Ambas funciones permiten que el chasis asigne direcciones WWN/MAC (Nombre mundial/Control de acceso de medios) a dispositivos Fibre Channel y Ethernet. Las direcciones WWN/MAC asignadas por el chasis son exclusivas a nivel mundial y específicas para una ranura de servidor.

Comparación entre FlexAddress y FlexAddress Plus

FlexAddress cuenta con 208 direcciones divididas en 16 ranuras de servidor, por lo que a cada ranura se le asignan 13 direcciones MAC.

FlexAddress Plus cuenta con 2928 direcciones divididas en 16 ranuras de servidor, por lo que a cada ranura se le asignan 183 direcciones MAC.

En la tabla a continuación se muestra la cantidad de direcciones MAC en ambas funciones.

Tabla 35. Suministro de direcciones MAC en FlexAddress y FlexAddress Plus

	Red Fabric A	Fabric B	Fabric C	Administración del iDRAC	Total de direcciones MAC
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

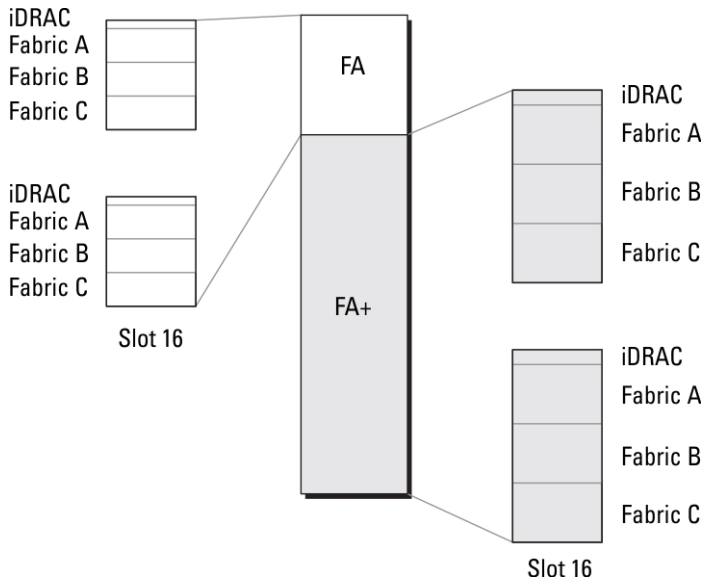


Ilustración 12. Funciones de FlexAddress (FA) y FlexAddress Plus (FA+)

Activación de FlexAddress

FlexAddress se presenta en una tarjeta Secure Digital (SD) que se debe insertar en la CMC para activar la función. Es posible que se requieran actualizaciones de software para activar la función FlexAddress; si no planea activar FlexAddress, estas actualizaciones no son necesarias. Las actualizaciones (que se muestran en la tabla a continuación) incluyen el BIOS de los módulos del servidor, el firmware o el BIOS de tarjetas mezzanine de E/S, y el firmware de la CMC. Aplique dichas actualizaciones antes de activar FlexAddress. De lo contrario, es posible que FlexAddress no funcione del modo esperado.

Tabla 36. Versiones mínimas de software para activar FlexAddress

Componente	Versión mínima necesaria
Tarjeta mezzanine Ethernet: Broadcom M5708t, 5709, 5710	• Firmware de código de inicio 4.4.1 o posterior • Firmware de inicio iSCSI 2.7.11 o posterior • Firmware de PXE 4.4.3 o posterior
Tarjeta mezzanine FC: QLogic QME2472, FC8	BIOS 2.04 o posterior
Tarjeta mezzanine FC: Emulex LPe1105-M4, FC8	BIOS 3.03a3 y firmware 2.72A2 o posterior
BIOS del módulo de servidor	• PowerEdge M600: BIOS 2.02 o posterior • PowerEdge M605: BIOS 2.03 o posterior • PowerEdge M805 • PowerEdge M905 • PowerEdge M610 • PowerEdge M710 • PowerEdge M710hd
LAN en placa base (LOM) de PowerEdgeM600/M605	• Firmware de código de inicio 4.4.1 o posterior • Firmware de inicio iSCSI 2.7.11 o posterior
iDRAC	• Versión 1.50 o posterior para sistemas PowerEdge xx0x • Versión 2.10 o posterior para sistemas PowerEdge xx1x
CMC	Versión 1.10 o posterior

NOTA: Todos los sistemas que se hayan solicitado después de junio de 2008 tendrán las versiones de firmware adecuadas.

Para asegurar la implementación correcta de la función FlexAddress, actualice el BIOS y el firmware en el orden siguiente:

1. Actualice el firmware y el BIOS de todas las tarjetas mezzanine.
2. Actualice el BIOS del módulo del servidor.
3. Actualice el firmware del iDRAC en el módulo del servidor.
4. Actualice el firmware de todos los CMC en el chasis; si hay CMC redundantes, asegúrese de que ambos estén actualizados.
5. En un sistema redundante de módulos CMC, inserte la tarjeta SD en el módulo pasivo o en el módulo CMC individual para un sistema no redundante.

   NOTA: Si el firmware del CMC que admite FlexAddress (versión 1.10 o posterior) no está instalado, no se activará la función.

   Consulte el documento *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification (Especificaciones técnicas de la tarjeta Secure Digital [SD] de Chassis Management Controller [CMC])* para obtener instrucciones de instalación de la tarjeta SD.

   NOTA: La tarjeta SD contiene la función FlexAddress. La información incluida en la tarjeta SD está cifrada, y no es posible duplicarla o alterarla de ninguna forma, porque esto podría afectar el funcionamiento del sistema y generar errores.

   NOTA: El uso de la tarjeta SD se limita a un solo chasis. Si tiene más de un chasis debe adquirir tarjetas SD adicionales.

   La activación de la función FlexAddress es automática cuando se reinicia la CMC con la tarjeta de función SD instalada; esta activación hará que la función se vincule al chasis actual. Si tiene la tarjeta SD instalada en la CMC redundante, la activación de la función FlexAddress no se produce hasta que la CMC redundante pase a ser la activa. Consulte el documento *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification (Especificaciones técnicas de la tarjeta Secure Digital [SD] de Chassis Management Controller [CMC])* para ver como convertir una CMC redundante en activa.

Cuando se reinicie la CMC, verifique el proceso de activación. Para obtener más información, consulte Verificación de la activación de FlexAddress.

Activación de FlexAddress Plus

FlexAddress Plus se proporciona en la tarjeta Secure Digital (SD) FlexAddress Plus junto con la función FlexAddress.

NOTA: La tarjeta SD denominada FlexAddress solamente contiene FlexAddress, mientras que la tarjeta denominada FlexAddress Plus contiene FlexAddress y FlexAddress Plus. La tarjeta debe estar colocada en la CMC para activar la función.

Es posible que algunos servidores, como PowerEdge M710HD, requieran más direcciones MAC de las que FA puede proporcionar a la CMC, según cómo estén configurados. En dichos servidores, al pasar a FA+ se puede optimizar por completo la configuración de WWN/MAC. Comuníquese con Dell para obtener asistencia en relación con la función FlexAddress Plus.

Para activar la función FlexAddress Plus se requieren las siguientes actualizaciones de software: BIOS del servidor, iDRAC del servidor y firmware de la CMC. Si estas actualizaciones no se aplican, solo estará disponible la función FlexAddress. Para obtener más información acerca de las versiones mínimas necesarias de estos componentes, consulte el archivo *Readme (Léame)*, disponible en **dell.com/support/manuals**.

Verificación de la activación de FlexAddress

Use el siguiente comando de RACADM para verificar la tarjeta de función SD y el estado de esta:

```
racadm featurecard -s
```

Tabla 37. Mensajes de estado que muestra el comando featurecard -s

Mensaje de estado	Acciones
No feature card inserted.	Revise la CMC para verificar que la tarjeta SD se ha insertado correctamente. En una configuración de CMC redundante, asegúrese de que la CMC con la tarjeta de función SD instalada sea la CMC activa y no la CMC en espera.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función está vinculada a este chasis.	No es necesario realizar ninguna acción.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función está vinculada a otro chasis svctag = ABC1234, SN de tarjeta SD = 01122334455	Retire la tarjeta SD; coloque e instale la tarjeta SD en el chasis actual.
La tarjeta de función insertada es válida y contiene las siguientes funciones de FlexAddress: la tarjeta de función no está vinculada a ningún chasis.	La tarjeta de función se puede mover a otro chasis o se puede reactivar en el chasis actual. Para reactivarla en el chasis actual, introduzca `racadm racreset` hasta que el módulo de la CMC con la tarjeta de función instalada se active.

Use el siguiente comando de RACADM para mostrar todas las funciones activadas en el chasis:

```
racadm feature -s
```

El comando produce el mensaje de estado siguiente:

```
Feature = FlexAddress
Date Activated = 8 April 2008 - 10:39:40
Feature installed from SD-card SN = 01122334455
```

Si no hay funciones activas en el chasis, el comando mostrará un mensaje:

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

Las tarjetas de funciones de Dell pueden contener más de una función. Una vez activada en un chasis alguna de las funciones de la tarjeta de función Dell, todas las demás funciones que se puedan incluir en la tarjeta no se podrán activar en un chasis diferente. En ese caso, el comando racadm feature -s mostrará el siguiente mensaje para las funciones afectadas:

```
ERROR: One or more features on the SD card are active on another chassis
```

Para obtener más información acerca de los comandos `feature` y `featurecard`, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos de Chassis Management Controller para Dell PowerEdge M1000e).

Desactivación de FlexAddress

Se puede desactivar la función FlexAddress y regresar la tarjeta SD a su estado previo a la instalación mediante un comando RACADM. No hay ninguna función de desactivación en la interfaz web. La desactivación regresa la tarjeta SD a su estado original, para que se pueda 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 que haya una tarjeta instalada o con una tarjeta de otro chasis, la función se desactivará y no se realizará ningún 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 la ejecución, el comando fallará y mostrará el siguiente mensaje de error:

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

Para obtener más información acerca del comando, consulte la sección del comando **feature** de *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

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: En esta sección, el término FlexAddress también hace referencia a FlexAddress Plus.

Adquiera e instale la actualización de FlexAddress para configurar FlexAddress. De lo contrario, aparecerá el siguiente texto en la interfaz web:

```
Optional feature not installed. See the Dell Chassis Management Controller Users Guide for
information on the chassis-based WWN and MAC address administration feature. To purchase this
feature, please contact Dell at www.dell.com.
```

Si adquirió FlexAddress con su chasis, ya está instalado y activo al encender el sistema. Si adquirió FlexAddress por separado, debe instalar la tarjeta de función SD siguiendo las instrucciones del documento *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification (Especificaciones técnicas de la tarjeta Secure Digital [SD] de Chassis Management Controller [CMC])*, disponible en **dell.com/support/manuals**.

El servidor debe apagarse 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 las redes Fabric que desee, puede seleccionar las ranuras que activará. Por ejemplo, si se activa la red Fabric A, todas las ranuras activadas tendrán FlexAddress activado solo en la red Fabric A. El resto de las redes Fabric utilizarán la WWN/MAC asignada de fábrica en el servidor.

Las ranuras seleccionadas tendrán FlexAddress activado para todas las redes Fabric activadas. Por ejemplo, no es posible activar las redes Fabric A y B, y activar FlexAddress para la ranura 1 en la red Fabric A pero no en la B.

NOTA: Asegúrese de que los servidores blade estén apagados antes de cambiar la dirección flexible de nivel de red Fabric (A, B, C o DRAC).

Conceptos relacionados

Encendido en LAN con FlexAddress en la página 176
Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis en la página 176
Configuración de FlexAddress para las ranuras en el nivel del servidor en la página 177
Configuración adicional de FlexAddress para Linux en la página 177

Encendido en LAN con FlexAddress

Cuando se implementa la función FlexAddress por primera vez en un módulo de servidor, se requiere de una secuencia de apagado y encendido para que FlexAddress se active. FlexAddress en dispositivos Ethernet se programa mediante el BIOS del módulo de servidor. Para que el BIOS del módulo de servidor programe la dirección, necesita estar en funcionamiento, lo cual requiere que el módulo de servidor se encienda. Cuando se completan las secuencias de apagado y encendido, las Id. de 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 servidor, puede activar o desactivar la función FlexAddress para redes Fabric y ranuras. FlexAddress se activa de forma individual en cada red Fabric y luego se seleccionan las ranuras que participarán en la función. Tanto las redes Fabric como las ranuras deben activarse para configurar FlexAddress satisfactoriamente.

Configuración de FlexAddress para redes Fabric y ranuras en el nivel del chasis mediante la interfaz web del CMC

Para activar o desactivar redes Fabric y ranuras para usar la función de FlexAddress mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Configuración** > **FlexAddress**.
   Aparecerá la página **Implementar FlexAddress**.
2. En la sección **Select Fabrics for Chassis-Assigned WWN/MACs (Seleccionar redes Fabric para WWN/MAC asignadas por el chasis)**, seleccione el tipo de red Fabric para la cual desea activar FlexAddress. Para desactivar esta opción, desmárquela.

   NOTA: Si no se seleccionan las redes Fabric, FlexAddress no estará activado para las ranuras seleccionadas.

   Aparecerá la página **Seleccionar ranuras para las WWN/MAC asignadas por el chasis**.
3. Seleccione la opción **Enabled (Activado)** para la ranura en la cual desea activar FlexAddress. Para desactivar esta opción, desmárquela.

   NOTA: Si un servidor está presente en la ranura, apáguelo antes de activar la función FlexAddress en esa ranura.

   NOTA: Si no se selecciona ninguna ranura, FlexAddress no estará activado para las redes Fabric seleccionadas.

4. Haga clic en **Aplicar** para guardar los cambios.
   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis mediante RACADM

Para activar o desactivar las redes Fabric, use el siguiente comando RACADM:

```
racadm setflexaddr [-f <fabricName> <state>]
```

donde `<fabricName> = A, B, C, or iDRAC` y `<state> = 0 or 1`

El valor 0 es desactivar y 1 es activar.

Para activar o desactivar las ranuras, use el siguiente comando RACADM:

```
racadm setflexaddr [-i <slot#> <state>]
```

donde `<slot#> = 1or 16` y `<state> = 0 or 1`

El valor 0 es desactivar y 1 es activar.

Para obtener más información sobre el comando **setflexaddr**, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*. en **dell.com/support/manuals**.

Configuración de FlexAddress para las ranuras en el nivel del servidor

En el nivel del servidor, puede activar o desactivar la función FlexAddress para ranuras individuales.

Configuración de FlexAddress para las ranuras en el nivel del servidor mediante la interfaz web del CMC

Para activar o desactivar una ranura individual y utilizar la función FlexAddress mediante la interfaz web del CMC:

1. En el árbol del sistema, expanda la opción **Descripción general del servidor**.
   Todos los servidores (de 1 a 16) aparecerán en la lista expandida **Servidores**.
2. Haga clic en el servidor que desea ver.
   Aparecerá la página **Estado del servidor**.
3. Haga clic en la ficha **Configuración** y en la subficha **FlexAddress**.
   Aparecerá la página **FlexAddress**.
4. En el menú desplegable **FlexAddress activada**, seleccione la opción **Sí** para activar la función FlexAddress o seleccione **No** para desactivarla.
5. Haga clic en **Aplicar** para guardar los cambios.
   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Configuración de FlexAddress para las ranuras en el nivel del servidor mediante RACADM

Para configurar FlexAddress para las ranuras en el nivel del servidor mediante RACADM:

```
racadm setflexaddr [-i <slot#> <state>] [-f <fabricName> <state>]
```

donde `<slot#> = 1 to 16`

`<fabricName> = A, B, C`

`<state> = 0 or 1`

El valor 0 es desactivar y 1 es activar.

Configuración adicional de FlexAddress para Linux

Cuando se cambia de una identificación MAC asignada por el servidor a una identificación MAC asignada por el chasis en sistemas operativos basados en Linux, es posible que se requieran pasos adicionales de configuración:

- SUSE Linux Enterprise Server 9 y 10: es posible que deba ejecutarse YAST (Yet Another Setup Tool) en el sistema Linux para configurar los dispositivos de red y después reiniciar los servicios de red.
- Red Hat Enterprise Linux 4 y Red Hat Enterprise Linux 5: Ejecute Kudzu, una utilidad para detectar y configurar hardware nuevo o modificado en el sistema. Kudzu mostrará el menú de detección de hardware; detecta el cambio en la dirección MAC, ya que se quitó y agregó hardware.

Visualización de la información de direcciones WWN o MAC

Puede ver el inventario de direcciones virtuales de los adaptadores de red de cada ranura de servidor o de todos los servidores del chasis. El inventario de direcciones virtuales incluye lo siguiente:

- Configuración de la red Fabric

  NOTA:
  - La red Fabric A muestra el tipo de red Fabric de entrada/salida instalado. Si está activada la red Fabric A, las ranuras que no están ocupadas muestran las direcciones MAC asignadas al chasis para la red Fabric A.
  - La controladora de administración de iDRAC no es una red Fabric, pero su FlexAddress es considerado como tal.
  - Una marca de verificación verde indica que la red Fabric está activada para FlexAddress o FlexAddressPlus.
- Protocolo que se está utilizando en el puerto del adaptador NIC. Por ejemplo, LAN, iSCSI, FCoE, etc.
- La configuración del nombre mundial (WWN) de Fiber Channel y las direcciones de control de acceso de medios (MAC) de una ranura en el chasis.
- Tipo de asignación de la dirección MAC y tipo de dirección activa actualmente: MAC asignada por el servidor, FlexAddress o de identidad de E/S. Una marca de verificación negra indica el tipo de dirección activa, ya sea asignada por el servidor, por el chasis o de forma 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. A partir de 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.

Usando la interfaz web, puede ver la información de las direcciones WWN/MAC de ranuras específicas mediante la página **FlexAddress** (haga clic en **Server Overview (Descripción general del servidor)** > **Slot <x> (Ranura <x>)** > **Setup (Configuración)** > **FlexAddress**). Puede ver la información de las direcciones WWN/MAC de todas las ranuras y del servidor desde la página **WWN/MAC Summary (Resumen de WWN/MAC)** (haga clic en **Server Overview (Descripción general del servidor)** > **Properties (Propiedades)** > **WWN/MAC**). Desde ambas páginas puede ver la información de direcciones WWN/MAC en el modo básico o en el modo avanzado:

- **Basic Mode (Modo básico)**: En este modo, puede ver la ranura del servidor, la red Fabric, el protocolo, las direcciones WWN/MAC y el estado de las particiones. 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.
- **Advanced Mode (Modo avanzado)**: En este modo, puede ver todos los campos que se muestran en el modo básico y todos los tipos de MAC (asignada por el servidor, Flex Address y de 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 **Expand/Collapse All (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 acerca de los campos, consulte la *ayuda en línea*.

Visualización de la información básica de las direcciones WWN o MAC mediante la interfaz web

Para ver la información de las direcciones WWN/MAC para cada ranura de servidor o todos los servidores del chasis en el modo básico:

1. Haga clic en **Descripción general del servidor** > **Propiedades** > **WWN/MAC**.
   La página **Resumen de WWN/MAC** muestra la información sobre las direcciones WWN/MAC.

Otra opción es hacer clic en **Server Overview (Descripción general del servidor)** > **Slot <x> (Ranura <x>)** > **Setup (Configuración)** > **FlexAddress** para ver la información de las direcciones WWN/ MAC de una ranura de 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 de una ranura o haga clic en **Expand/Collapse All (Expandir/contraer todo)** para expandir o contraer los atributos de una ranura específica o todas las ranuras en la tabla de 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. En el menú desplegable **Protocolo**, seleccione **Todos los protocolos** o uno de los protocolos de red de la lista para ver todas las direcciones MAC 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. Otra opción es introducir parcialmente la dirección MAC para ver las ranuras asociadas. Por ejemplo, introduzca 4A para ver las ranuras con las direcciones MAC que contienen 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 acerca de los campos, consulte la *ayuda en línea*.

Visualización de la información avanzada de las direcciones WWN o MAC mediante la interfaz web

Para ver información sobre las direcciones WWN/MAC para cada ranura de servidor o todos los servidores del chasis en el modo avanzado:

1. Haga clic en **Descripción general del servidor** > **Propiedades** > **WWN/MAC**.
   La página **Resumen de WWN/MAC** muestra la información sobre las direcciones WWN/MAC.
2. En el menú desplegable **Ver** , seleccione **Opciones avanzadas** para ver los atributos de las direcciones WWN/MAC en la vista detallada.
   En la tabla **WWN/MAC Addresses (Direcciones WWN/MAC)** se presentan la ranura del servidor, la red Fabric, el protocolo, las direcciones WWN/MAC, el estado de la partición y el tipo de dirección MAC activa actualmente: asignada por el servidor, FlexAddress o de identidad de E/S. Una marca de verificación negra indica el tipo de dirección activa, ya sea asignada por el servidor, por el chasis o de forma remota. MAC. Si un servidor no tiene activado el tipo FlexAddress o de identidad de E/S, el estado de **FlexAddress (Chassis-Assigned) (FlexAddress, asignada por el chasis)** o **I/O Identity (Remote-Assigned) (Identidad de E/S, asignada en forma remota)** se muestra como **Not Enabled (No activado)**, pero la marca de verificación negra indica asignada por el servidor.
3. En la tabla **Direcciones WWN/MAC** , haga clic en **Exportar** para guardar las direcciones WWN/MAC localmente.
4. Haga clic en el de una ranura o haga clic en **Expand/Collapse All (Expandir/contraer todo)** para expandir o contraer los atributos de una ranura específica o todas las ranuras en la tabla de 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. En el menú desplegable **Protocolo**, seleccione **Todos los protocolos** o uno de los protocolos de red de la lista para ver todas las direcciones MAC 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. Otra opción es introducir parcialmente la dirección MAC para ver las ranuras asociadas. Por ejemplo, introduzca 4A para ver las ranuras con las direcciones MAC que contienen 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 acerca de los campos, consulte la *ayuda en línea*.

Visualización de la información de direcciones WWN o MAC mediante RACADM

Para ver la información de las direcciones WWN/MAC para todos los servidores o servidores específicos mediante RACADM, utilice los subcomandos `getflexaddr` y `getmacaddress`.

Para mostrar Flexaddress para todo el chasis, utilice el siguiente comando RACADM:

```
racadm getflexaddr
```

Para ver el estado de FlexAddress para una ranura particular, utilice el siguiente comando de RACADM:

```
racadm getflexaddr [-i <slot#>]
```

donde *<n.º de ranura>* es un valor entre 1 y 16.

Para ver la dirección MAC de la LOM o NDC, utilice el siguiente comando de RACADM:

```
racadm getmacaddress
```

Para ver la dirección MAC del chasis, utilice el siguiente comando RACADM:

```
racadm getmacaddress -m chassis
```

Para ver las direcciones MAC de iSCSI de todos los servidores, utilice el siguiente comando de RACADM:

```
racadm getmacaddress -t iscsi
```

Para ver las MAC de iSCSI para un servidor específico, utilice el siguiente comando de RACADM:

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

Para ver la dirección MAC y WWN definida por el usuario, utilice el siguiente comando de RACADM:

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

Para ver la MAC/WWN asignada por la consola de todas las LOM o tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c all
```

Para ver la dirección asignada WWN/MAC del chasis, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c flexaddress
```

Para ver la direcciones MAC/WWN para todas las LOM o tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c factory
```

Para ver las direcciones MAC/WWN de iSCSI y Ethernet para todos los iDRAC/LOM/tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -a
```

Para obtener más información acerca de los subcomandos `getflexaddr` y `getmacaddress`, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACAMD de Chassis Management Controller para Dell PowerEdge M1000e).

Visualización del nombre mundial o la Id. de control de acceso de medios

La página **WWN/MAC Summary (Resumen de WWN/MAC)** permite ver la configuración de nombre mundial (WWN) y la dirección de control de acceso de medios (MAC) de una ranura del chasis.

Configuración de la red Fabric

La sección **Fabric Configuration (Configuración de la red Fabric)** muestra el tipo de red Fabric de entrada/salida instalada para la red Fabric A, la B y la C. Una marca verde indica que la red Fabric está activada para FlexAddress. La función FlexAddress se utiliza para implementar direcciones WWN/MAC de ranuras fijas y asignadas por el chasis en varias redes Fabric y ranuras dentro del chasis. Esta función se activa según la red Fabric y la ranura.

NOTA: Para obtener más información acerca de la función FlexAddress, consulte Acerca de FlexAddress.

Direcciones WWN o MAC

La sección **Dirección WWN/MAC** muestra información de WWN/MAC que se asigna a todos los servidores, aunque esas ranuras del servidor se encuentren vacías actualmente.

- **Location (Ubicación)** muestra la ubicación de la ranura ocupada por los módulos de E/S. Las seis ranuras se identifican con una combinación del nombre de grupo (A, B o C) y el número de ranura (1 o 2): A1, A2, B1, B2, C1 o C2. iDRAC es la controladora de administración integrada del servidor.
- **Red Fabric** muestra el tipo de red Fabric de E/S.
- **Asignadas por el servidor** muestra las direcciones WWN/MAC asignadas por el servidor integradas en el hardware de la controladora.
- **Asignadas por el chasis** muestra las direcciones WWN/MAC asignadas por el chasis que se utilizan para la ranura particular.

Una marca verde en las columnas **Server-Assigned (Asignadas por el servidor)** y **Chassis-Assigned (Asignadas por el chasis)** indica el tipo de direcciones activas. Las direcciones asignadas por el chasis se asignan cuando se activa FlexAddress en el chasis y representan las direcciones de ranura fija. Cuando se seleccionan las direcciones asignadas por el chasis, esas direcciones se utilizarán aunque se sustituya un servidor por otro.

Mensajes de comandos

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

Tabla 38. Comandos y mensajes de salida de FlexAddress

Situación	Comando	Salida
La tarjeta SD en el módulo CMC activo está vinculada a otra etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: The feature card is bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`
La tarjeta SD en el módulo CMC activo está vinculada a la misma etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: The feature card is bound to this chassis`

Tabla 38. Comandos y mensajes de salida de FlexAddress (continuación)

Situación	Comando	Salida
La tarjeta SD en el módulo CMC activo no está vinculada a ninguna etiqueta de servicio.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: The feature card is not bound to any chassis`
Función FlexAddress no activada en el chasis por algún motivo (no hay tarjeta SD insertada, tarjeta SD dañada, después haber desactivado la función, tarjeta SD vinculada a otro chasis).	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotstate>]`	`ERROR: Flexaddress feature is not active on the chassis`
El usuario invitado intenta configurar FlexAddress en ranuras o redes Fabric.	`$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`

CONTRATO DE LICENCIA DE SOFTWARE DE DELL FlexAddress

El presente documento es un contrato legal entre usted, el usuario, y Dell Products, L.P. o Dell Global B.V. ("Dell"). Este contrato cubre a todo el software que se distribuye con el producto Dell, para el cual no existe ningún contrato de licencia aparte entre usted y el fabricante o el propietario del software (colectivamente, el "Software"). Este contrato no es para la venta de Software ni ninguna 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 este contrato son derechos reservados para el fabricante o propietario del Software. Al abrir o romper el sello de los paquetes de Software, instalar o descargar el Software, o utilizar el Software precargado 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 del Software (discos, material escrito y embalaje) y elimine todo el Software precargado o incluido.

Puede utilizar cada copia del Software solamente en un equipo a la vez. Si dispone de varias licencias del Software, podrá utilizar a la vez tantas copias como licencias tenga. Por "utilizar" se entiende cargar el Software en la memoria temporal o en el almacenamiento permanente del equipo. La instalación en un servidor de red únicamente para la distribución a otros equipos no es "utilizar" si (pero solo si) usted dispone de una licencia diferente para cada equipo donde se distribuya el Software. Debe asegurarse de que la cantidad de personas que utilicen el Software instalado en un servidor de red no sea superior a la cantidad de licencias de las que disponga. Si la cantidad de usuarios del Software instalado en un servidor de red supera la cantidad de licencias, deberá adquirir licencias adicionales hasta que la cantidad de licencias sea igual a la cantidad de usuarios, antes de permitir que utilicen el Software. Si usted es cliente comercial de Dell o filial de Dell, por el presente concede a Dell, o a un representante seleccionado por Dell, el derecho a realizar una auditoría del uso que usted hace del Software durante el horario laboral normal, acepta cooperar con Dell en dicha auditoría y acepta proporcionarle a Dell todos los registros relacionados razonablemente con el uso que usted hace del Software. La auditoría se limitará a la verificación del cumplimiento por su parte de los términos de este contrato.

El Software está protegido por las leyes de derechos de autor de Estados Unidos y por los tratados internacionales. Puede hacer una copia del Software únicamente para disponer de una copia de seguridad o archivo, o puede transferirla a un solo disco duro siempre y cuando guarde el original únicamente para disponer de una copia de seguridad o archivo. No puede alquilar ni arrendar el Software 240 mediante tarjetas FlexAddress y FlexAddress Plus ni copiar los materiales escritos que se adjuntan con el Software, pero sí puede transferir el Software y todos los materiales adjuntos de manera definitiva como parte de la venta o transferencia del producto Dell, siempre y cuando

no se quede con ninguna copia y el destinatario acepte los términos de este documento. Toda transferencia debe incluir la actualización más reciente y todas las versiones anteriores. No puede aplicar técnicas de ingeniería inversa, descompilar ni desensamblar el Software. Si el paquete que acompaña a su equipo contiene discos compactos, o disquetes de 3,5" o 5,25", puede utilizar únicamente los adecuados para su equipo. No puede utilizar los discos en ningún otro equipo o red, prestarlos, alquilarlos, arrendarlos ni 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 ni de mano de obra con el uso normal durante los noventa (90) días posteriores a la recepción por parte de usted. Esta garantía se limita a usted y no es transferible. Las garantías implícitas se limitan a los noventa (90) días posteriores a la fecha de recepción del Software. Algunas jurisdicciones no permiten limitaciones en la vigencia de las garantías implícitas, de modo que esta limitación quizás no se aplique en su caso. La responsabilidad total de Dell y de sus proveedores, y la reparación exclusiva, se limitarán a (a) la devolución del importe pagado por el Software o (b) la sustitución de los discos que no cumplan con esta garantía enviados a Dell con un número de autorización de devolución haciéndose cargo usted del costo y riesgo del envío. Esta garantía limitada se anulará si el disco se daña como resultado de accidentes, abusos, aplicaciones no adecuadas, o mantenimiento o modificaciones por parte de alguna persona ajena a Dell. Los discos de reemplazo poseen garantía por el tiempo más largo entre el período restante de la garantía original y los treinta (30) días posteriores al reemplazo.

Dell NO garantiza que las funciones del Software satisfarán sus necesidades ni que el funcionamiento del Software será sin interrupciones y errores. Usted asume la responsabilidad de seleccionar el Software en busca de los resultados que usted espera, y asume la responsabilidad del uso y los resultados obtenidos con el Software.

DELL, EN NOMBRE PROPIO Y DE SUS PROVEEDORES, DESCONOCE TODAS LAS DEMÁS GARANTÍAS, EXPLÍCITAS O IMPLÍCITAS, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN PROPÓSITO DETERMINADO EN LO QUE SE REFIERE AL SOFTWARE Y A TODOS LOS MATERIALES ESCRITOS QUE LO ACOMPAÑAN. Esta garantía limitada le otorga derechos legales específicos, aunque usted puede tener otros que varían según la jurisdicción.

EN NINGÚN CASO, DELL NI SUS PROVEEDORES SERÁN RESPONSABLES POR NINGÚN DAÑO EN ABSOLUTO (LO QUE INCLUYE, ENTRE OTROS, LOS DAÑOS POR PÉRDIDA DE GANANCIAS COMERCIALES, INTERRUPCIÓN DE ACTIVIDAD COMERCIAL, PÉRDIDA DE INFORMACIÓN COMERCIAL O CUALQUIER OTRA PÉRDIDA PECUNIARIA) A CAUSA DEL USO O LA INCAPACIDAD DE UTILIZAR EL SOFTWARE, AUNQUE SE NOTIFIQUE LA POSIBILIDAD DE TALES DAÑOS. Dado que algunas jurisdicciones no permiten la exclusión o limitación de la responsabilidad por daños consecuentes o accidentales, la limitación anterior quizás no se aplique a usted.

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 SEA ÚTIL, PERO SE PROPORCIONA EN SU ESTADO ACTUAL SIN NINGUNA GARANTÍA EXPLÍCITA NI IMPLÍCITA; INCLUIDA, ENTRE OTRAS, LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. BAJO NINGUNA CIRCUNSTANCIA, DELL, LOS TITULARES DE LOS DERECHOS INTELECTUALES NI LOS COLABORADORES SERÁN RESPONSABLES POR DAÑOS DIRECTOS, INDIRECTOS, ACCIDENTALES, ESPECIALES, EJEMPLARES O CONSECUENTES (LO QUE INCLUYE, ENTRE OTROS, LA ADQUISICIÓN DE SERVICIOS O PRODUCTOS SUSTITUTOS; LA PÉRDIDA DE USO, DATOS O GANANCIAS; O LA INTERRUPCIÓN DE LA ACTIVIDAD COMERCIAL) SIN IMPORTAR LA CAUSA NI LA TEORÍA DE RESPONSABILIDAD, YA SEA POR CONTRATO, RESPONSABILIDAD ESTRICTA O EXTRACONTRACTUAL (INCLUIDA LA NEGLIGENCIA Y OTROS) QUE SE HAYAN OCASIONADO POR EL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ SOBRE LA POSIBILIDAD DE DICHO DAÑO.

DERECHOS LIMITADOS DEL GOBIERNO DE EE.UU.

El software y la documentación son "artículos comerciales", tal como se define dicho término en 48 C.F.R. 2.101, que constan de "software informático comercial" y "documentación de software informático comercial", tal como se utilizan dichos términos en 48 C.F.R. 12.212. En 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 este documento.

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

GENERAL

Esta licencia estará en vigor hasta que finalice. Dicha finalización se dará según las condiciones estipuladas anteriormente o si usted no cumple con alguno de estos términos. Una vez finalizada, usted acepta que se procederá a la destrucción del Software, los materiales que lo acompañan y 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, según lo máximo permitido por la ley, a todo derecho a un juicio con jurado con respecto al Software o este contrato. Dado que esta renuncia puede no aplicarse en ciertas jurisdicciones, es posible que no se aplique a usted. Usted reconoce que ha leído el presente contrato, lo entiende, acepta estar sujeto a sus términos, y esta es la declaración completa y exclusiva del contrato entre usted y Dell con respecto al Software.

13

Admin de fabric de entrada y salida

El chasis puede tener hasta seis módulos de I/O (IOM), en los que cada IOM es un módulo de switch o paso. Los IOM se clasifican en tres grupos: A, B y C. Cada grupo tiene dos ranuras: ranura 1 y ranura 2.

Las ranuras se designan con letras, de izquierda a derecha, en la parte trasera del chasis: A1 | B1 | C1 | C2 | B2 | A2. Cada servidor tiene ranuras para dos tarjetas mezzanine (MC) para conectarse a los IOM. La MC y el IOM correspondiente deben tener el mismo fabric.

La IO del chasis se clasifica en tres rutas de datos discretas: A, B y C. Estas rutas se describen como FABRICS y son compatibles con Ethernet, Fibre Channel o InfiniBand. Estas rutas de fabric discretas se dividen en dos bancos de IO, banco uno y banco dos. Cada adaptador de IO del servidor (tarjeta mezzanine o LOM) puede tener dos o cuatro puertos en función de la capacidad. Estos puertos se dividen uniformemente en bancos uno y dos de IOM para permitir la redundancia. Cuando implemente las redes Ethernet, iSCSI o Fibre Channel, incluya sus enlaces redundantes en los bancos uno y dos para obtener la máxima disponibilidad. El IOM discreto se identifica con el identificador de fabric y el número de banco.

Ejemplo: A1 denota Fabric A en el Banco 1. C2 denota Fabric Cin en el Banco 2.

El chasis admite tres tipos de fabric o protocolo. Los IOM y las tarjetas mezzanine en un grupo deben tener los mismos tipos de fabric o unos que sean compatibles.

- Los IOM del Grupo A están siempre conectados a los adaptadores Ethernet integrados del servidor; por lo tanto, el tipo de fabric del Grupo A siempre será Ethernet.
- En el Grupo B, las ranuras de los IOM están conectadas permanentemente a la primera ranura de la MC de cada módulo del servidor.
- En el Grupo C, las ranuras de los IOM están conectadas permanentemente a la segunda MC de cada módulo del servidor.

NOTA: En la CLI del CMC, se hace referencia a los IOM mediante la convención, switch-n: A1 = switch-1, A2 = switch-2, B1 = switch-3, B2 = switch-4, C1 = switch-5 y C2 = switch-6.

Conceptos relacionados

Descripción general de la administración de redes Fabric en la página 185
Configuraciones no válidas en la página 186
Situación de encendido por primera vez en la página 186
Supervisión de la condición del módulo de E/S en la página 186
Configuración de los valores de red para módulos de E/S en la página 188
Administración de VLAN para módulos de E/S en la página 191
Administración de las operaciones de control de alimentación para módulos de E/S en la página 195
Activación o desactivación del parpadeo del LED para los módulos de E/S en la página 195

Tareas relacionadas

Restablecimiento de los módulos de E/S a la configuración predeterminada de fábrica en la página 189

Temas:

- Administración de las operaciones de control de alimentación para módulos de E/S
- Activación o desactivación del parpadeo del LED para los módulos de E/S

Descripción general de la administración de redes Fabric

La administración de redes Fabric ayuda a evitar problemas relacionados con la electricidad, las configuraciones o la conectividad debido a la instalación de un módulo de E/S o una MC con un tipo de red Fabric incompatible con el tipo de red Fabric establecido del chasis. Las configuraciones no válidas de hardware pueden provocar problemas eléctricos u operativos en el chasis o sus componentes. La administración de redes Fabric evita que se activen configuraciones no válidas.

En la siguiente figura se muestra la ubicación de los módulos de E/S en el chasis. La ubicación de cada módulo de E/S se indica con su número de grupo (A, B o C). Estas rutas de redes Fabric independientes se dividen en dos bancos de E/S: banco uno y dos. En el chasis, los nombres de las ranuras de los módulos de E/S se identifican como A1, A2, B1, B2, C1 y C2.

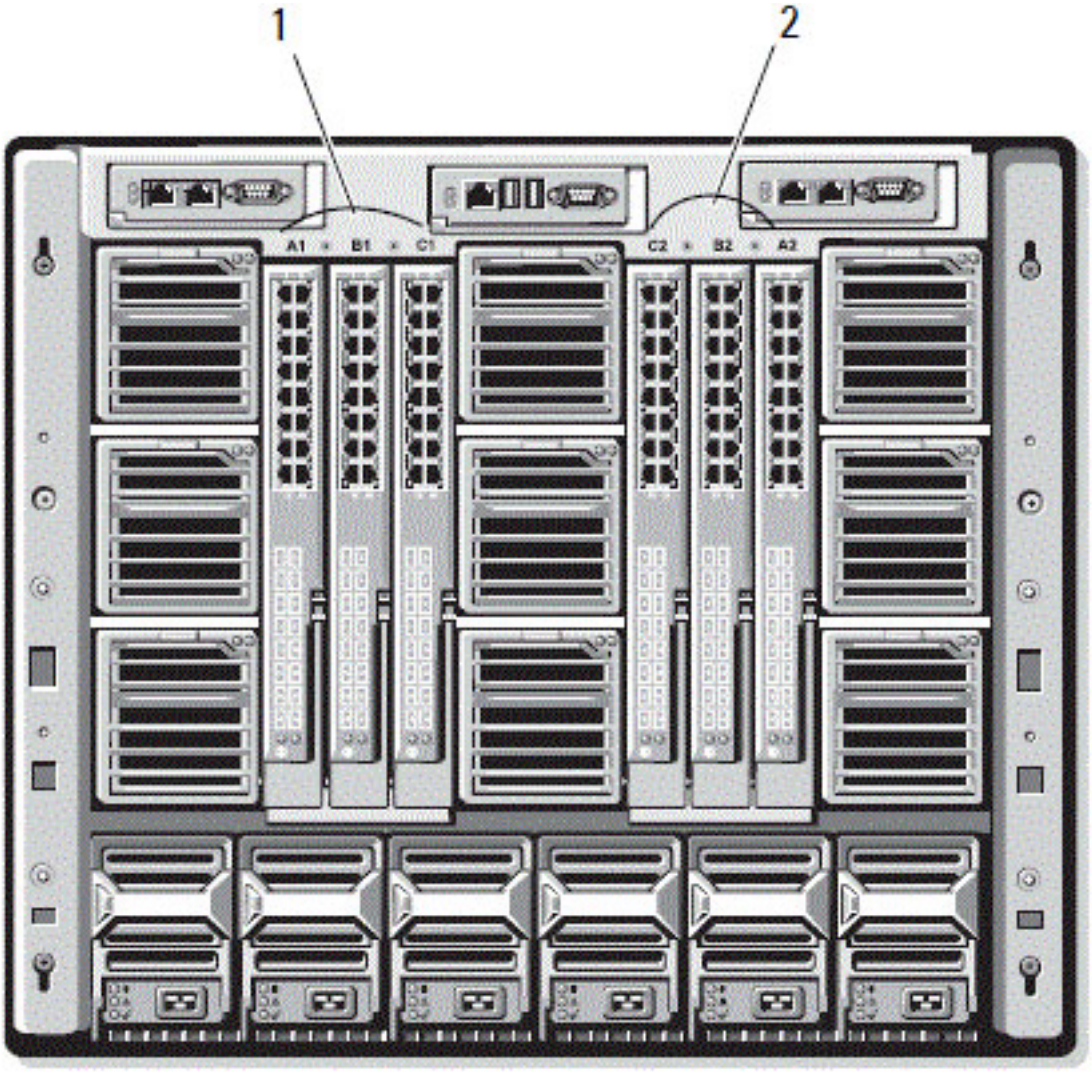


Ilustración 13. Vista posterior de un chasis, que muestra la ubicación de los módulos de E/S

Tabla 39. Ubicaciones de los módulos de E/S en la parte posterior de un chasis

1	Banco 1 (ranuras A1, B1, C1)	2	Banco 2 (ranuras A2, B2, C2)

El CMC crea anotaciones en el registro de hardware y en los registros del CMC para las configuraciones de hardware no válidas.

Por ejemplo:

- Una MC Ethernet conectada a un módulo de E/S Fibre Channel es una configuración no válida. No obstante, una MC Ethernet conectada a un conmutador Ethernet y a un módulo de E/S de paso Ethernet instalados en el mismo grupo de módulos de E/S es una conexión válida.
- Un módulo de E/S de paso Fibre Channel y un módulo de E/S de conmutador Fibre Channel en las ranuras B1 y B2 es una configuración válida si las primeras MC en todos los servidores son también Fibre Channel. En este caso, la CMC activa los módulos de E/S y los servidores. No obstante, es posible que determinado software de redundancia Fibre Channel no admita esta configuración; no todas las configuraciones válidas son necesariamente configuraciones admitidas.

  La verificación de redes Fabric para MC y módulos de E/S de servidores se realiza solo cuando el chasis está encendido. Cuando el chasis está en espera, las iDRAC en los módulos del servidor permanecen apagados y, por ende, no pueden informar el tipo de red Fabric de la MC del servidor. Es posible que el tipo de red Fabric de la MC no se informe en la interfaz de usuario de la CMC hasta que la iDRAC del servidor esté encendida. Además, si el chasis está encendido, la verificación de redes Fabric se realiza cuando se inserta un servidor o módulo de E/S (opcional). Si se detecta una incompatibilidad de redes Fabric, el servidor o el módulo de E/S puede encenderse y el LED de estado parpadea en color ámbar.

Configuraciones no válidas

Hay tres tipos de configuraciones no válidas:

- Configuración no válida de MC o LOM, donde el tipo de red Fabric recién instalado del servidor es diferente a la red Fabric del módulo de E/S existente; es decir, que el LOM o la MC de un servidor no es compatible con el módulo de E/S correspondiente. En este caso, el resto de los servidores del chasis funcionan, pero el servidor con la tarjeta MC incompatible no puede encenderse. El botón de encendido del servidor parpadea en ámbar para alertar de una incompatibilidad de red Fabric.
- Configuración no válida de módulo de E/S-MC, donde el tipo de red Fabric recién instalado del módulo de E/S y los tipos de red Fabric de la MC residente no coinciden o son incompatibles. El módulo de E/S incompatible se mantiene en el estado apagado. La CMC agrega una entrada a los registros de la CMC y el hardware, para indicar la configuración no válida y especificar el nombre del módulo de E/S. La CMC hace parpadear el LED de error en el módulo de E/S con problemas. Si la CMC está configurada para enviar alertas, enviará alertas de correo electrónico y SNMP por este suceso.
- Configuración no válida entre módulos de E/S, donde un módulo de E/S recién instalado tiene un tipo de red Fabric incompatible o diferente a la de un módulo de E/S ya instalado en su grupo. La CMC mantiene el módulo de E/S recién instalado en estado apagado, hace parpadear el LED de error del módulo de E/S, y agrega entradas relativas a la incompatibilidad en los registros de la CMC y el hardware.

Situación de encendido por primera vez

Cuando el chasis se conecta y se enciende, los módulos de E/S tienen prioridad sobre los servidores. Se permite al primer módulo de E/S de cada grupo encenderse antes que los demás. En este momento, no se realiza la verificación de sus tipos de red Fabric. Si no hay ningún módulo de E/S en la primera ranura de un grupo, se enciende el módulo de la segunda ranura del grupo. Si ambas ranuras tienen módulos de E/S, se compara el módulo de la segunda con el módulo de la primera para ver si son congruentes.

Después de que los módulos de E/S se encienden, los servidores se encienden y el CMC verifica si las redes Fabric de los servidores son congruentes.

Se permite un conmutador y un módulo de paso en el mismo grupo, siempre y cuando sus redes Fabric sean idénticas. Puede haber conmutadores y módulos de paso en el mismo grupo, aunque sean fabricados por proveedores distintos.

Supervisión de la condición del módulo de E/S

Para obtener información sobre la supervisión de la condición del módulo de E/S, consulte Viewing Information and Health Status of All IOMs (Visualización de información y estado de condición de todos los módulos de E/S) y Viewing Information and Health Status For Individual IOM (Visualización de información y estado de condición de un módulo de E/S individual).

Visualización del estado de los enlaces ascendente y descendente del módulo de entrada/salida mediante la interfaz web

Puede ver la información de estado del enlace ascendente y del enlace descendente del agregador de E/S Dell PowerEdge M con la interfaz web del CMC:

1. Diríjase a **Descripción general del chasis** y expanda **Descripción general del módulo de E/S** en el árbol del sistema.
   Aparecerán todos los módulos de E/S (1–6) en la lista expandida.
2. Haga clic en el módulo de E/S (ranura) que desea ver S
   Aparecerá la página **I/O Module Status (Estado del módulo de E/S)** de la ranura del módulo específica. Se presentarán las tablas **I/O Module Uplink Status (Estado de enlace ascendente del módulo de E/S)** y **I/O Module Downlink Status (Estado de enlace descendente del módulo de E/S)**. Estas tablas muestran información sobre los puertos de enlace descendente (1–32) y los puertos de enlace ascendente (33–56). Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
   NOTA: Asegúrese de que el agregador de E/S tenga configuraciones válidas para que el estado del enlace del puerto sea activo. Esta página muestra el estado del agregador de E/S. Si el estado es inactivo, los puertos del servidor en el agregador de E/S pueden estar inactivos debido a configuraciones no válidas.

Visualización de la información de sesión de FCoE de los módulos de E/S mediante la interfaz web

Puede ver la información de la sesión de FCoE del agregador de E/S Dell PowerEdge M con la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Descripción general del chasis** y expanda **Descripción general del módulo de E/S**.
   Aparecerán todos los módulos de E/S (1–6) en la lista expandida.
2. Haga clic en el módulo de E/S (ranura) que desee ver y haga clic en **Properties (Propiedades)** > **FCoE**.
   Aparecerá la página **Módulo de E/S 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 sección **Información de la sesión de FCoE** mostrará la información de la sesión de FCoE del conmutador.
   NOTA: Esta sección muestra la información de FCoE solo si las sesiones de FCoE activas se están ejecutando en el agregador de E/S.

Visualización de la información de apilamiento del agregador de entrada/salida Dell PowerEdge M

Puede visualizar la siguiente información de apilamiento en el agregador de E/S Dell PowerEdge M con el comando `racadm getioinfo`:

- ID de apilamiento: esta es la dirección MAC del maestro de apilamiento que identifica el apilamiento asociado con este módulo.
- Unidad de apilamiento: este es un número entero que identifica la posición del agregador de E/S en el apilamiento.
- ID del chasis: esta ID ayuda a describir la topología física de un apilamiento e identifica la ubicación de un conmutador en particular.
- Función de apilamiento: Esto identifica la función de este módulo en el apilamiento. Los valores válidos son Master (Maestro), Member (Miembro) y Standby (En espera).

El comando `racadm getioinfo` con la opción -s le permite visualizar la información de apilamiento relacionada del agregador de E/S para los conmutadores presentes en el chasis y sus unidades apiladas, tanto en el chasis local como en el chasis externo.

Use el siguiente comando para visualizar la información de apilamiento para los conmutadores solo en el chasis local:

```
racadm getioinfo -s
```

Use el siguiente comando para visualizar la información de apilamiento de las unidades apiladas locales y también las unidades en el chasis externo:

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

Consulte la sección del comando `racadm getioinfo` en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

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 el valor de red, es necesario tener:

- Privilegios de administrador para la red Fabric A, para configurar módulos de E/S en el grupo A.
- Privilegios de administrador para la red Fabric B, para configurar módulos de E/S en el grupo B.
- Privilegios de administrador para la red Fabric C, para configurar módulos de E/S en el grupo C.

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 provoca que no se configure la dirección IP fuera de banda. Consulte la documentación del módulo de E/S para ver la dirección IP de administración en banda predeterminada.

NOTA: No intente configurar los valores de la red del módulo de E/S para módulos de paso de Ethernet y conmutadores de Infiniband.

Configuración de los valores de red para los módulos de E/S mediante la interfaz web del CMC

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

Para configurar los valores de red de los módulos de E/S mediante la interfaz web de la 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**, 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. Para los módulos de E/S requeridos, active DHCP, escriba la dirección IP, la máscara de subred y la dirección de la puerta de enlace.
3. Para los módulos de E/S que se pueden administrar, introduzca la contraseña raíz, la cadena de comunidad SNMP RO y la dirección IP del servidor Syslog. Para obtener información sobre los campos, consulte *CMC Online Help (Ayuda en línea de la CMC)*.

   NOTA: La dirección IP establecida en los módulos de E/S de la CMC no se guarda en la configuración de inicio permanente del conmutador. Para guardar la configuración de la dirección IP de forma definitiva, debe introducir el comando RACADM `connect switch-n command` o `racadm connect switch -n`, o bien usar una interfaz directa a la GUI del módulo de E/S para guardar esta dirección en el archivo de configuración de inicio.

   NOTA: La cadena de comunidad SNMP puede tener cualquier carácter imprimible cuyo valor ASCII se encuentre en el rango 33-125.

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

   NOTA: Para los módulos de E/S que se pueden administrar, es posible restablecer las VLAN, las propiedades de red y los puertos de E/S a las configuraciones predeterminadas.

Configuración de los valores de red para los módulos de E/S mediante RACADM

Para configurar los valores de la red de los módulos de E/S mediante RACADM, establezca la fecha y la hora. Consulte la sección del comando `deploy` en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

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-<n> -u root -p <password>
```

```
racadm deploy -m switch-<n> -v SNMPv2 <snmpCommunityString> ro
```

```
racadm deploy -a [server|switch] -u root -p <password>
```

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 mediante la página **Implementar módulos de E/S**.

NOTA: Esta función solo se admite en el módulo de E/S Agregador de E/S PowerEdge M. 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 la opción **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.

Conceptos relacionados

Descripción general de la administración de redes Fabric en la página 185
Configuraciones no válidas en la página 186
Situación de encendido por primera vez en la página 186
Supervisión de la condición del módulo de E/S en la página 186
Configuración de los valores de red para módulos de E/S en la página 188
Administración de VLAN para módulos de E/S en la página 191
Administración de las operaciones de control de alimentación para módulos de E/S en la página 195
Activación o desactivación del parpadeo del LED para los módulos de E/S en la página 195

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

Para actualizar el software de módulos de E/S, seleccione la imagen de software que desee en una ubicación especificada. También puede regresar a una versión de software anterior.

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

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 lo contrario, desplácese a cualquiera de las siguientes páginas:

- **Descripción general del chasis** > **Actualizar**
- **Descripción general del chasis** > **Controladora del chasis** > **Actualizar**
- **Descripción general del chasis** > **iKVM** > **Actualizar**

Aparece la página **Actualización de firmware**, que proporciona un vínculo para acceder a la página **Actualización del firmware del módulo de E/S**.

2. En la página **Actualización del firmware del módulo de E/S**, en la sección **Firmware del módulo de E/S**, 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 la actualización de software utilizando la opción **Browse (Examinar)**. El nombre de la imagen de software se ve en el campo **IOM Software Location (Ubicación de software de módulo de E/S)**.
   En la sección **Update Status (Estado de actualización)** se 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.

   Una vez finalizada la actualización o reversión, se produce una pérdida breve de conectividad en el dispositivo de módulo de E/S debido a su reinicio y se muestra el nuevo firmware en la página **Firmware y software 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 del agregador de E/S (IOA GUI)

Puede iniciar la GUI del agregador de E/S (IOA) desde la CMC para administrar la configuración del IOA. Para iniciar la GUI del IOA desde la CMC, el módulo de E/S debe estar configurado en IOA y usted debe tener privilegios de administrador para la red Fabric A, B o C.

Puede iniciar la GUI del agregador de E/S (IOA GUI) 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 IOA por primera vez, se le solicitará que personalice la contraseña.

Inicio de la GUI del agregador de E/S (IOA GUI) desde la página Descripción general del chasis

Vaya a **Chassis Overview (Descripción general del chasis)** > **Quick Links (Vínculos de acceso rápido)** > **Launch I/O Module GUI (Iniciar GUI del módulo de E/S)**. Aparecerá la página de inicio de sesión del IOA.

Inicio de la GUI del agregador de E/S (IOA GUI) desde la página Descripción general del módulo de E/S

En el árbol de directorios, vaya a **I/O Module Overview (Descripción general del módulo de E/S)**. En la página **I/O Module Status (Estado del módulo de E/S)**, haga clic en **Launch I/O Module GUI (Iniciar GUI del módulo de E/S)**. Aparecerá la página de inicio de sesión del IOA.

Inicio de la GUI del agregador de E/S (IOA GUI) desde la página Estado del módulo de E/S

En el árbol de directorios, en **I/O Module Overview (Descripción general del módulo de E/S)**, haga clic en un agregador de E/S. En la página **I/O Module Status (Estado del módulo de E/S)**, haga clic en **Launch I/O Module GUI (Iniciar GUI del módulo de E/S)**.

Módulo del Agregador de Entrada/Salida

Puede ver los detalles del módulo de E/S y de los módulos flexibles en el RACADM de la CMC y las páginas **Condición del chasis**, **Estado del módulo de E/S** y **Descripción general del módulo de E/S**.

La CMC informa sobre los módulos flexibles en el Agregador de E/S al leer la información del módulo flexible durante su negociación inicial con el Agregador de E/S. La lectura se produce mediante el envío de comandos XML durante la negociación inicial. La CMC guarda la información del módulo flexible en la memoria compartida. Puede haber un máximo de dos módulos flexibles:

- Módulo de E/S flexible 1
- Módulo de E/S flexible 2

Todo software del módulo de E/S que admite la revisión 4 del comando admite el comando XML de la información del módulo de E/S flexible. La CMC envía la información del módulo flexible solo si la versión de la revisión del comando es 4 o posterior. Cualquier error de lectura de la información del módulo flexible se almacena en el registro del chasis.

La información del módulo flexible puede tener los siguientes cinco valores:

- Módulo de E/S flexible 4x de 10 G base = 0
- Módulo de E/S flexible 4x de 10 G SFP+ = 1
- Módulo de E/S flexible 2x de 40 G QSFP+ = 2
- Módulo de E/S flexible 4xFC = 3
- No hay ningún módulo flexible instalado = 4

Cualquier valor mayor que 4 se considera inválido. La CMC muestra el módulo flexible como "Inválido/desconocido".

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

- Independiente
- VLT
- 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.

Administración de VLAN para módulos de E/S

Las LAN virtuales (VLAN) para los módulos de E/S le permiten separar a los usuarios en segmentos de red individuales por cuestiones de seguridad y otros motivos. Al usar VLAN, puede aislar las redes para usuarios individuales en un conmutador de 32 puertos. Puede asociar puertos seleccionados en un conmutador con VLAN seleccionadas y considerar a estos puertos un conmutador diferente.

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

Después de cambiar el modo del agregador de E/S de apilamiento a independiente, elimine 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.

Tareas relacionadas

Configuración de los valores de VLAN en los módulos de E/S mediante la interfaz web del CMC en la página 193
Visualización de los valores de VLAN en los módulos de E/S mediante la interfaz web del CMC en la página 193
Visualización de la configuración actual de VLAN en los módulos de E/S mediante la interfaz web del CMC en la página 194
Adición de VLAN etiquetadas para los módulos de E/S mediante la interfaz web del CMC en la página 194
Eliminación de las VLAN para los módulos de E/S mediante la interfaz web del CMC en la página 194
Actualización de VLAN sin etiquetar para módulos de E/S mediante la interfaz web del CMC en la página 194
Restablecimiento de las VLAN para módulos de E/S mediante la interfaz web del CMC en la página 195

Configuración de la VLAN de administración en módulos de E/S con la interfaz web

Puede administrar el agregador de E/S dentro de banda a través de una VLAN. Esta VLAN debe implementarse antes de su uso. La CMC permite la implementación de una VLAN de administración dentro de banda. La VLAN de administración dentro de banda del conmutador requiere que se aplique la siguiente configuración básica de opciones:

- Activar
- ID de VLAN
- Priority

NOTA:

La configuración de la VLAN de administración en la página **Vlan Settings (Configuración de Vlan)** requiere privilegios de **configuración del chasis**. Este privilegio también se requiere para la configuración de VLAN de módulos de E/S, además de los privilegios de **administrador** para la red Fabric específica A, B o C.

Para configurar la VLAN de administración en el módulo de E/S con la interfaz web del CMC:

1. En el árbol del sistema, diríjase a **Descripción general del chasis** y haga clic en **Red** > **VLAN**.
   Aparecerá la página **Configuración de la etiqueta VLAN**.
2. En la sección **I/O Modules (Módulos de E/S)**, active la VLAN para los módulos de E/S, establezca la prioridad e introduzca la Id.
   Para obtener más información acerca de los campos, consulte *CMC Online Help (Ayuda en línea de la CMC)*.
3. Haga clic en **Aplicar** para guardar la configuración.

Configuración de la VLAN de administración en módulos de E/S con RACADM

Para configurar la VLAN de administración en módulos de E/S con RACADM, use el comando `racadm setniccfg -m switch-n -v .`

- Especifique la identificación y la prioridad de VLAN de un módulo de E/S específico con el siguiente comando:

  ```
  racadm setniccfg -m switch -<n> -v <VLAN id> <VLAN priority>
  ```

  Los valores válidos para `<n>` son 1-6.

  Los valores válidos para `<VLAN>` son 1-4000 y 4021-4094. El valor predeterminado es 1.

  Los valores válidos para `<VLAN priority>` son 0-7. El valor predeterminado es 0.

  Por ejemplo:

  ```
  racadm setniccfg -m switch -1 -v 1 7
  ```

  Por ejemplo:

  ```
  ```

- Para eliminar la VLAN de un módulo de E/S, desactive las capacidades de VLAN de la red del módulo de E/S especificado:

  ```
  racadm setniccfg -m switch-<n> -v
  ```

Los valores válidos para <n> son 1-6.

Por ejemplo:

```
racadm setniccfg -m switch-1 -v
```

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

NOTA: Puede configurar los valores de VLAN solo en el módulo de E/S (IOM) Agregador de E/S PowerEdge M. No se admiten otros módulos de E/S, como MXL 10/40GbE.

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

1. En el árbol del sistema, 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 **Paso 1: Seleccionar módulos de E/S**, seleccione el tipo de configuración en la lista desplegable y, a continuación, seleccione los módulos de E/S requeridos.

   Para obtener información sobre los campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*
3. En la sección **Paso 2: Especificar rango de puerto**, seleccione el rango de puertos de redes Fabric que desea asignar a los módulos de E/S seleccionados.

   Para obtener información sobre los campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*
4. Seleccione la opción **Seleccionar** o **Deseleccionar todo** para aplicar los cambios a todos los módulos de E/S o a ninguno.

   o

   Active la casilla de las ranuras específicas para seleccionar los módulos de E/S requeridos.
5. En la sección **Step 3: Edit VLANs (Paso 3: Editar las VLAN)**, introduzca las Id. de VLAN de los IOM. Indique un valor entre 1 y 4094. Las Id. de VLAN se pueden introducir como un rango o separadas por coma. Ejemplo: 1,5,10,100-200.
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**.

   Para obtener información sobre los campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*

   NOTA: En la sección Summary VLANs of All Ports (Resumen de VLAN de todos los puertos), se muestra información sobre los IOM presentes en el chasis y las VLAN asignadas. Haga clic en Save (Guardar) para guardar un archivo csv del resumen de la configuración de VLAN actual.

   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 del CMC

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

1. En el árbol del sistema, 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 del CMC

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

1. En el árbol del sistema, vaya a **I/O Module Overview (Descripción general del módulo de E/S)** y haga clic en **Setup (Configuración)** > **VLAN Manager (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**.
   Aparecerá el mensaje Operation Successful (Operación correcta). La configuración actual de VLAN asignada a los módulos de E/S se mostrará en el campo VLAN Assignment Summary (Resumen de asignaciones de VLAN).

Adición de VLAN etiquetadas para los módulos de E/S mediante la interfaz web del CMC

Para agregar VLAN etiquetadas para los módulos de E/S 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** > **Administrador de VLAN**.
   Aparecerá la página Administrador de VLAN.
2. En la sección **Paso 1: Seleccionar módulo de E/S**, seleccione los módulos de E/S requeridos.
3. En la sección **Paso 2: Especificar rango de puerto**, seleccione el rango de puertos de redes Fabric que desea asignar a los módulos de E/S seleccionados.

   Para obtener información sobre los campos, consulte *CMC Online Help* (Ayuda en línea para el CMC).
4. Seleccione la opción **Seleccionar** o **Deseleccionar todo** para aplicar los cambios a todos los módulos de E/S o a ninguno.

   o

   Active la casilla de las ranuras específicas para seleccionar los módulos de E/S requeridos.
5. En la sección **Paso 3: Editar VLAN**, seleccione **Agregar VLAN etiquetadas** en la lista desplegable y haga clic en **Aplicar**.

   Las VLAN etiquetadas se asignan a los módulos de E/S seleccionados.

   Aparecerá el mensaje Operation Successful (Operación correcta). La configuración actual de VLAN asignada a los módulos de E/S se mostrará en el campo **VLAN Assignment Summary (Resumen de asignaciones de VLAN)**.

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

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

1. En el árbol del sistema, 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 **Paso 1: Seleccionar módulo de E/S**, seleccione los módulos de E/S requeridos.
3. En la sección **Paso 3: 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.

   Aparecerá el mensaje Operation Successful (Operación correcta). La configuración actual de VLAN asignada a los módulos de E/S se mostrará en el campo **VLAN Assignment Summary (Resumen de asignaciones de VLAN)**.

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

Para actualizar VLAN sin etiquetar para módulos de E/S 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** > **Administrador de VLAN**.

Aparecerá la página **Administrador de VLAN**.

2. En la sección **Paso 1: Seleccionar módulo de E/S**, seleccione los módulos de E/S requeridos.
3. En la sección **Paso 2: Especificar rango de puerto**, seleccione el rango de puertos de redes Fabric que desea asignar a los módulos de E/S seleccionados.

   Para obtener información sobre los campos, consulte *CMC Online Help* (Ayuda en línea para el CMC).
4. Seleccione la opción **Seleccionar/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 **Paso 3: 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 **OK** (Aceptar) para confirmar.

   Las VLAN sin etiquetar se actualizarán con las configuraciones de la VLAN sin etiquetar recientemente asignada.

   Aparecerá el mensaje Operation Successful (Operación correcta). La configuración actual de VLAN asignada a los módulos de E/S se mostrará en el campo VLAN Assignment Summary (Resumen de asignaciones de VLAN).

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

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

1. En el árbol del sistema, 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 **Paso 1: Seleccionar módulo de E/S**, seleccione los módulos de E/S requeridos.
3. En la sección **Paso 3: 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 **OK** (Aceptar) para confirmar.

   Las VLAN se asignarán a los módulos de E/S seleccionados de acuerdo con las configuraciones predeterminadas.

   Aparecerá el mensaje Operation Successful (Operación correcta). La configuración actual de VLAN asignada a los módulos de E/S se mostrará en el campo **VLAN Assignment Summary (Resumen de asignaciones de VLAN)**.

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

Administración de las operaciones de control de alimentación para módulos de E/S

Para obtener información para establecer la operación de control de alimentación para uno o varios módulos de E/S, consulte Executing Power Control Operations on an IOM (Ejecución de las operaciones de control de alimentación en un módulo de E/S).

Activación o desactivación del parpadeo del LED para los módulos de E/S

Para obtener información sobre cómo activar el parpadeo del LED para los módulos de E/S, consulte Configuring LEDs to Identify Components on the Chassis (Configuración de los LED para identificar componentes en el chasis).

14

Configuración y uso de iKVM

El módulo KVM de acceso local para el chasis del servidor Dell M1000e se denomina módulo de conmutador KVM integrado Avocent o iKVM. El iKVM es un conmutador analógico de teclado, video y mouse que se conecta en el chasis. Es un módulo opcional de acoplamiento activo para el chasis que ofrece acceso local de teclado, mouse y video a los servidores del chasis y a la línea de comandos de la CMC activa.

Conceptos relacionados

Interfaz de usuario del iKVM en la página 196
Funciones clave de iKVM en la página 196
Interfaces de conexión física en la página 197

Temas:

Interfaz de usuario del iKVM

El iKVM utiliza la interfaz gráfica de usuario de Reporte y configuración en pantalla (OSCAR), que se activa mediante una tecla de acceso rápido. OSCAR permite seleccionar uno de los servidores o la línea de comandos de Dell CMC donde desee acceder por medio del teclado, la pantalla y el mouse locales. Se permite solo una sesión de iKVM por chasis.

Conceptos relacionados

Uso de la interfaz OSCAR en la página 197

Funciones clave de iKVM

- Seguridad: Protege el sistema con una contraseña de protector de pantalla. Después de un tiempo definido por el usuario, se activa el modo de protector de pantalla y se deniega el acceso hasta que se introduzca la contraseña correcta para reactivar OSCAR.
- Exploración: permite seleccionar una lista de servidores, que aparecen en el orden seleccionado mientras OSCAR se encuentra en el modo de exploración.
- Identificación del servidor: La CMC asigna nombres de ranuras exclusivos para todos los servidores del chasis. Si bien es posible asignar nombres a los servidores mediante la interfaz de OSCAR desde una conexión categorizada, prevalecerán los nombres asignados por la CMC, y todos los nombres nuevos que se asignen a los servidores mediante OSCAR se sobrescribirán.

  Para cambiar los nombres de las ranuras con la interfaz web de la CMC, consulte Configuración de nombres de las ranuras. Para cambiar el nombre de una ranura mediante RACADM, consulte la sección **setslotname** en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.
- Video: las conexiones de video del iKVM admiten resoluciones de pantalla de video de entre 640 x 480 a 60 Hz y 1280 x 1024 a 60 Hz.
- Plug and Play: el iKVM admite el uso de la función Plug and Play de canal de datos para la pantalla (DDC), que automatiza la configuración del monitor de video y cumple con la norma VESA DDC2B.
- Actualización: Permite actualizar el firmware del iKVM mediante la interfaz web de la CMC o el comando `fwupdate` de RACADM.

Conceptos relacionados

Uso de la interfaz OSCAR en la página 197
Admin de servidores con iKVM en la página 201
Admin del iKVM desde el CMC en la página 208
Actualización de firmware del iKVM en la página 48

Interfaces de conexión física

Es posible conectarse a un servidor o a la consola CLI del CMC a través del módulo iKVM desde el panel frontal del chasis, una interfaz de consola analógica (ACI) o el panel posterior del chasis.

NOTA: Los puertos del panel de control situado en la parte frontal del chasis están específicamente diseñados para el iKVM, que es opcional. Si no se tiene el módulo de iKVM, no podrán utilizarse los puertos del panel de control frontal.

Prioridades de las conexiones del iKVM

Solo hay una conexión de iKVM disponible por vez. El iKVM asigna un orden de prioridad para cada tipo de conexión, de modo que cuando hay varias conexiones solo una está disponible mientras que las otras están desactivadas.

El orden de prioridad de las conexiones del iKVM es el siguiente:

1. Panel frontal
2. ACI
3. Panel posterior

Por ejemplo, si tiene conexiones de iKVM en el panel frontal y ACI, la conexión del panel frontal permanecerá activa, mientras que la conexión de ACI quedará desactivada. Si tiene conexiones en el panel posterior y ACI, tiene prioridad la de ACI.

Categorización por medio de la conexión de ACI

El iKVM admite conexiones categorizadas con servidores y la consola de línea de comandos de la CMC para el iKVM, ya sea de forma local a través de un puerto de conmutador de consola remota o de manera remota a través del software Dell RCS. El iKVM admite conexiones de ACI de los siguientes productos:

- Dell Remote Console Switch 180AS, 2160AS, 2161DS*, 2161DS-2 o 4161DS
- Sistema de conmutación Avocent AutoView
- Sistema de conmutación Avocent DSR
- Sistema de conmutación Avocent AMX

NOTA: 2161 DS no admite la conexión de Dell CMC Console.

NOTA: El iKVM también admite una conexión de ACI con los modelos Dell 180ES y 2160ES, aunque la categorización no es óptima. Esta conexión requiere un SIP de USB a PS2.

Uso de la interfaz OSCAR

Esta sección proporciona información para iniciar, configurar y usar la interfaz OSCAR.

Conceptos relacionados

Inicio de OSCAR en la página 197
Conceptos básicos de navegación en la página 198
Configuración de OSCAR en la página 199

Inicio de OSCAR

Para iniciar OSCAR:

1. Presione <Impr Pant>.
   Se muestra el cuadro de diálogo **Principal**.

   Si hay asignada una contraseña, aparecerá el cuadro de diálogo **Contraseña** después de hacer clic en <Impr Pant>.
2. Escriba la contraseña y haga clic en **Aceptar**.
   Aparecerá el cuadro de diálogo **Principal**.

   NOTA: Existen cuatro opciones para invocar OSCAR. Puede activar una, varias o todas estas secuencias de teclas; para ello, seleccione las casillas de la sección Invoke OSCAR (Invocar OSCAR) del cuadro de diálogo Main (Principal).

Conceptos relacionados

Configuración de la seguridad de la consola en la página 203
Conceptos básicos de navegación en la página 198

Conceptos básicos de navegación

Tabla 40. : Navegación por OSCAR con el teclado y el mouse

Tecla o secuencia de teclas	Resultado
• <Impr Pant>-<Impr Pant> • <Mayús>-<Mayús> • <Alt>-<Alt> • <Ctrl>-<Ctrl>	Cualquiera de estas secuencias de teclas abre OSCAR según la configuración de **Invoke OSCAR (Invocar OSCAR)**. Puede activar dos, tres o todas estas secuencias de teclas si selecciona las casillas en la sección **Invoke OSCAR (Invocar OSCAR)** del cuadro de diálogo **Main (Principal)** y luego hace clic en **OK (Aceptar)**.
<F1>	Abre la pantalla **Ayuda** del cuadro de diálogo actual.
<Esc>	Cierra el cuadro de diálogo actual sin guardar los cambios y regresa al cuadro de diálogo anterior. En el cuadro de diálogo **Principal**, la tecla <Esc> cierra la interfaz OSCAR y regresa al servidor seleccionado. En un cuadro de mensaje, cierra el cuadro emergente y regresa al cuadro de diálogo actual.
<Alt>	Abre cuadros de diálogo, selecciona o marca opciones y ejecuta acciones cuando se utiliza en combinación con letras subrayadas u otros caracteres designados.
<Alt>+<X>	Cierra el cuadro de diálogo actual y regresa al cuadro de diálogo anterior.
<Alt>+<O>	Selecciona la opción **Aceptar** y regresa al cuadro de diálogo anterior.
<Intro>	Completa una operación de conmutación en el cuadro de diálogo **Principal** y sale de OSCAR.
Hacer clic, <Intro>	En un cuadro de texto, selecciona el texto para editar, y activa las teclas de flecha izquierda y derecha para desplazar el cursor. Presione <Intro> nuevamente para salir del modo de edición.
<Impr Pant>, <Retroceso>	Vuelve a la selección anterior si no hubo otras pulsaciones de teclas.
<Impr Pant>, <Alt>+<0>	Desconecta de inmediato a un usuario de un servidor; no se selecciona ningún servidor. El indicador de estado señala Free (Libre). Esta acción solo se aplica al =<0> del teclado y no al del teclado numérico.
<Impr Pant>, <Pausa>	Enciende el modo de protector de pantalla inmediatamente e impide el acceso a esa consola, si se encuentra protegida con contraseña.
Teclas de flecha hacia arriba/ abajo	Desplazan el cursor de línea en línea en las listas.
Teclas de flecha hacia la derecha/la izquierda	Desplazan el cursor entre las columnas al editar un cuadro de texto.
<Inicio>/<Fin>	Desplazan el cursor hacia la parte superior (Inicio) o inferior (Fin) de una lista.
<Supr>	Elimina caracteres en un cuadro de texto.
Teclas de números	Permite ingresar datos desde el teclado principal o el teclado numérico.
<Bloq Mayús>	Deshabilitada Para pasar de mayúsculas a minúsculas o viceversa, utilice la tecla <Mayús>.

Configuración de OSCAR

Es posible configurar los valores de OSCAR mediante el cuadro de diálogo **Configuración**.

Acceso al cuadro de diálogo Configuración

Para obtener acceso al cuadro de diálogo **Configuración**:

1. Presione <Impr Pant> para iniciar la interfaz OSCAR.
   Se muestra el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración**.
   Se muestra el cuadro de diálogo **Configuración**.

Tabla 41. Cuadro de diálogo Configuración: funciones

Función	Propósito
Menú	Ordena la lista de servidores por número de ranura o alfabéticamente por nombre.
Seguridad	• Define una contraseña para restringir el acceso a los servidores. • Activa un protector de pantalla y define un periodo de inactividad antes de que el protector aparezca y se establezca el modo de protección de pantalla.
Indicador	Cambia la imagen, la duración, el color o la ubicación del indicador de estado.
Idioma	Cambia el idioma de todas las pantallas de OSCAR.
Difusión	Se configura para controlar varios servidores de forma simultánea a través de acciones del teclado o el mouse.
Exploración	Define un patrón de exploración personalizado para un máximo de 16 servidores.

Tareas relacionadas

Cambio de comportamiento del modo de visualización en la página 199
Asignación de secuencias de teclas para OSCAR en la página 199
Configuración del tiempo de retraso de la pantalla en la interfaz OSCAR en la página 200
Configuración de la visualización del indicador de estado en la página 200

Cambio de comportamiento del modo de visualización

Use el cuadro de diálogo **Menú** para cambiar el orden de visualización de los servidores y definir un tiempo de retraso de pantalla para OSCAR.

Para cambiar el comportamiento del modo de visualización:

1. Presione <Impr Pant> para iniciar OSCAR.
   Aparecerá el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración** y después en **Menú**.
   Aparecerá el cuadro de diálogo **Menú**.
3. Para elegir el orden de visualización predeterminado de los servidores, realice uno de los siguientes pasos:
   - Seleccione **Nombre** para visualizar los servidores ordenados alfabéticamente en función del nombre.
   - Seleccione **Ranura** para visualizar los servidores ordenados por número de ranura.
4. Haga clic en **OK** (Aceptar).

Asignación de secuencias de teclas para OSCAR

Para asignar una o varias secuencias de teclas para la activación de OSCAR, seleccione una secuencia de teclas en el menú **Invoke OSCAR (Invocar OSCAR)** y haga clic en **OK (Aceptar)**. La tecla predeterminada para invocar OSCAR es <Impr Pant>.

Configuración del tiempo de retraso de la pantalla en la interfaz OSCAR

Para establecer un tiempo de retraso de la pantalla en la interfaz OSCAR, presione <Impr Pant>, escriba el número de segundos (0 a 9) que durará el retraso de la pantalla en OSCAR y haga clic en **Aceptar**.

Si introduce el valor <0> OSCAR se abrirá sin retraso.

El tiempo de retraso de la pantalla de OSCAR permite realizar una conmutación mediante software.

Conceptos relacionados

Conmutación mediante software en la página 202

Configuración de la visualización del indicador de estado

El indicador de estado aparece en el escritorio y muestra el nombre del servidor seleccionado o el estado de la ranura seleccionada. Utilice el cuadro de diálogo Flag (Indicador) para ordenar la información por servidor, o para cambiar el color del indicador, la opacidad, la duración y la ubicación en el escritorio.

Tabla 42. Visualización del indicador

Indicador	Descripción
	Tipo de indicador por nombre.
	Señala que el usuario está desconectado de todos los sistemas.
	Indica que el modo de transmisión se encuentra activado.

Para configurar la visualización del indicador de estado:

1. Presione <Impr Pant> para iniciar OSCAR.
   Aparecerá el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración** y después en **Indicador**.
   Aparecerá el cuadro de diálogo **Indicador**.
3. Seleccione **En pantalla** para mostrar el indicador todo el tiempo o bien, **En pantalla** y **Por tiempo** para mostrar el indicador solo durante cinco segundos después de la conmutación.

   NOTA: Si selecciona solo la opción **Por tiempo**, el indicador no se mostrará.
4. En la sección **Display Color (Color de visualización)**, seleccione un color para el indicador. Las opciones son negro, rojo, azul y púrpura.
5. En **Modo de visualización**, seleccione **Opaco** para que el color del indicador sea oscuro o **Transparente** para ver el escritorio a través del indicador.
6. Para definir la posición del indicador en el escritorio, haga clic en **Definir posición**.
   Se mostrará el indicador **Definir posición**.
7. Haga clic con el botón izquierdo del mouse en la barra de título y arrástrela hasta la ubicación deseada en el escritorio y, a continuación, haga clic con el botón derecho para regresar al cuadro de diálogo **Indicador**.
8. Haga clic en **Aceptar** y nuevamente en **Aceptar** para guardar la configuración.

   Para salir sin guardar los cambios, haga clic en el  .

Admin de servidores con iKVM

El iKVM es una matriz de switch analógico que admite hasta 16 servidores. El switch iKVM utiliza la interfaz de usuario de OSCAR para seleccionar y configurar los servidores. Además, el iKVM incluye una entrada del sistema para establecer una conexión de la consola de línea de comandos del CMC al CMC.

Si tiene una sesión activa de redirección de consola activa y un monitor de menor resolución está conectado al iKVM, la resolución de la consola del servidor puede restablecerse si se selecciona el servidor en la consola local. Si el servidor ejecuta un sistema operativo Linux, es posible que una consola X11 no esté visible en el monitor local. Si presiona <Ctrl><Alt><F1> en el iKVM, Linux se cambia a una consola de texto.

Conceptos relacionados

Compatibilidad con periféricos en la página 201
Visualización y selección de servidores en la página 201

Compatibilidad con periféricos

El módulo iKVM es compatible con los siguientes periféricos:

- Teclados USB de PC estándar con diseño QWERTY, QWERTZ, AZERTY y japonés 109.
- Monitores VGA con compatibilidad para DDC.
- Dispositivos señaladores USB estándares.
- Concentradores USB 1.1 con alimentación propia conectados al puerto USB local del iKVM.
- Concentradores USB 2.0 con alimentación conectados a la consola del panel frontal del chasis Dell M1000e.

NOTA: Puede utilizar varios teclados y mouse en el puerto USB local del iKVM. El iKVM acumula las señales de entrada. Si existen señales de entrada simultáneas de varios mouse o teclados USB, los resultados pueden ser impredecibles.

NOTA: Las conexiones USB sirven únicamente para teclados, mouse y concentradores USB compatibles. El iKVM no admite datos transmitidos desde otros periféricos USB.

Visualización y selección de servidores

Cuando inicia OSCAR, aparece el cuadro de diálogo **Main (Principal)**. Utilice el cuadro de diálogo **Main (Principal)** para ver, configurar y administrar servidores a través del iKVM. Los servidores se pueden ver por nombre o por ranura. El número de ranura corresponde al número de la ranura del chasis ocupada por el servidor. La columna **Slot (Ranura)** indica el número de ranura donde está instalado el servidor.

NOTA: La línea de comandos de Dell CMC ocupa la ranura 17. Si selecciona esta ranura se mostrará la línea de comandos de la CMC, donde podrá ejecutar comandos RACADM o conectarse a la consola serie de servidores o módulos de E/S.

NOTA: A los nombres y los números de ranura de los servidores los asigna el CMC.

Conceptos relacionados

Conmutación mediante software en la página 202

Tareas relacionadas

Visualización del estado del servidor en la página 201
Selección de servidores en la página 202

Visualización del estado del servidor

La columna de la derecha del cuadro de diálogo **Main (Principal)** indica el estado del servidor en el chasis. En la siguiente tabla se describen los símbolos de estado.

Tabla 43. Símbolos de estado de la interfaz OSCAR

Símbolos	Descripción
	El servidor está en línea.
	El servidor está fuera de línea o no se encuentra en el chasis.
	El servidor no está disponible.
	Se obtuvo acceso al servidor mediante el canal de usuario indicado con la letra: • A=panel posterior • B=panel frontal

Selección de servidores

Utilice el cuadro de diálogo **Main (Principal)** para seleccionar los servidores. Cuando selecciona un servidor, el iKVM reconfigura el teclado y el mouse con los valores apropiados para ese servidor.

- Para seleccionar los servidores, realice uno de los siguientes pasos:
  - Haga doble clic en el nombre del servidor o el número de ranura.
  - Si los servidores están ordenados por ranura (es decir, si el botón Ranura está presionado), escriba el número de ranura y presione <Intro>.
  - Si los servidores están ordenados por nombre (es decir, si el botón Nombre está presionado), escriba los primeros caracteres del nombre del servidor, defínalo como exclusivo y presione <Intro> dos veces.
- Para seleccionar al servidor anterior, presione <Impr Pant> y después <Retroceso>. Esta combinación de teclas permite alternar entre la conexión actual y la anterior.
- Para desconectar el usuario de un servidor, realice uno de los siguientes pasos:
  - Presione <Impr Pant> para acceder a OSCAR y haga clic en Desconectar.
  - Presione <Impr Pant> y, a continuación, <Alt> <0>. De esta forma queda con estado libre, sin servidores seleccionados. Si el indicador de estado del escritorio está activo, mostrará el estado Free (Libre). Consulte **Configuración de la visualización del indicador de estado**

Conmutación mediante software

La conmutación mediante software permite cambiar de un servidor a otro por medio de una secuencia de teclas. Presione la tecla <Impr Pant> para realizar una conmutación por software a un servidor y, a continuación, escriba los primeros caracteres de su nombre o número. Si anteriormente ha establecido un tiempo de retraso (el número de segundos antes de que el cuadro de diálogo **Main [Principal]** se muestra después de presionar <Impr Pant>) y pulsa la secuencia de teclas antes de que haya transcurrido ese tiempo, la interfaz OSCAR no se mostrará.

Tareas relacionadas

Configuración de la conmutación mediante software en la página 202
Conmutación mediante software a un servidor en la página 203

Configuración de la conmutación mediante software

Para configurar OSCAR para la conmutación mediante software:

1. Presione <Impr Pant> para iniciar la interfaz OSCAR.
   Aparecerá el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración** y después en **Menú**.
   Aparece el cuadro de diálogo **Menú**.
3. Seleccione **Nombre** o **Ranura** para la clave de orden/visualización.
4. Escriba el tiempo de retraso deseado expresado en segundos en el campo **Tiempo de retraso de pantalla**.
5. Haga clic en **OK** (Aceptar).

Conmutación mediante software a un servidor

Para realizar una conmutación mediante software a un servidor:

- Para seleccionar un servidor, presione <Impr Pant>. Si optó por que los servidores se ordenen por ranura, es decir, si el botón Slot (Ranura) está presionado, escriba el número de ranura y presione <Intro>.

  o

  Si los servidores aparecen ordenados por nombre según la opción elegida (es decir, si el botón Nombre está presionado), escriba los primeros caracteres del nombre del servidor para establecerlo como exclusivo y presione <Intro>.

- Para volver al servidor anterior, presione <Impr Pant> y después <Retroceso>.

Conexiones de video

El iKVM tiene conexiones de video en los paneles frontal y posterior del chasis. Las señales de conexión del panel frontal tienen prioridad respecto de las del panel posterior. Cuando se conecta un monitor al panel frontal, la conexión de video no se transmite al panel posterior, y aparece un mensaje de OSCAR para indicar que las conexiones de ACI y KVM del panel posterior quedan desactivadas. Si el monitor se desactiva (es decir, si se quita del panel frontal o se desactiva mediante un comando de la CMC), la conexión de ACI se activa, mientras que la de KVM del panel posterior permanece desactivada.

Conceptos relacionados

Prioridades de las conexiones del iKVM en la página 197
Activación o desactivación del acceso al iKVM desde el panel frontal en la página 208

Aviso de apropiación

Normalmente, un usuario conectado a una consola de servidor a través del iKVM y otro usuario conectado a la misma consola a través de la función de redirección de consola de la interfaz web del iDRAC tienen el mismo acceso a la consola y pueden escribir de forma simultánea.

Para evitar esta situación, antes de iniciar la redirección de consola de la interfaz web de la iDRAC, el usuario remoto puede desactivar la consola local en dicha interfaz. El usuario del iKVM local ve un mensaje de OSCAR que indica que se apropiará la conexión dentro de un tiempo determinado. El usuario local debería terminar de usar la consola antes de que finalice la conexión del iKVM con el servidor.

No existe una función de apropiación disponible para el usuario del iKVM.

NOTA: Si un usuario remoto de la iDRAC desactivó el video local de un servidor, las funciones de video, teclado y mouse de ese servidor no estarán disponibles para el iKVM. El estado del servidor aparecerá marcado con un punto amarillo en el menú de OSCAR para indicar que se encuentra bloqueado o no disponible para uso local. Consulte Visualización del estado del servidor.

Tareas relacionadas

Visualización del estado del servidor en la página 201

Configuración de la seguridad de la consola

OSCAR le permite configurar valores de seguridad en la consola del iKVM. Puede establecer un modo de protector de pantalla que se iniciará cuando la consola permanezca inactiva durante un plazo determinado. Cuando se inicia el modo, la consola permanece bloqueada hasta que se presiona una tecla o se mueve el mouse. Para continuar, es necesario introducir la contraseña del protector de pantalla.

Use el cuadro de diálogo **Seguridad** para bloquear la consola con una contraseña, establecer o cambiar la contraseña o activar el protector de pantalla.

NOTA: Si pierde u olvida la contraseña del iKVM, puede restablecerla a los valores predeterminados de fábrica de iKVM por medio de la interfaz web del CMC o RACADM.

Tareas relacionadas

Acceso al cuadro de diálogo Seguridad en la página 204
Configuración de la contraseña en la página 204
Protección por contraseña de la consola en la página 204

Acceso al cuadro de diálogo Seguridad

Para acceder al cuadro de diálogo **Seguridad**:

1. Presione <Impr Pant>.
   Aparecerá el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración** y, a continuación, en **Seguridad**.
   Aparecerá el cuadro de diálogo **Seguridad**.

Configuración de la contraseña

Para establecer la contraseña:

1. Haga clic una vez y presione <Intro> o haga doble clic en el campo **Nueva**.
2. Escriba la contraseña nueva y presione <Intro>. En las contraseñas se distingue entre mayúsculas y minúsculas, y deben usarse entre 5 y 12 caracteres. Deben incluir al menos una letra y un número. Los caracteres válidos son: A-Z, a-z, 0-9, espacio y guión.
3. Escriba nuevamente la contraseña en el campo **Repetir** y presione <Intro>.
4. Haga clic en **Aceptar** y cierre el cuadro de diálogo.

Protección por contraseña de la consola

Para proteger con contraseña la consola:

1. Establezca la contraseña como se describe en Setting Password (Configuración de la contraseña).
2. Seleccione la casilla **Activar protector de pantalla**.
3. Escriba la cantidad de minutos de **Tiempo de inactividad** (de 1 a 99) para retrasar la protección por contraseña y la activación del protector de pantalla.
4. Para **Modo**: si el monitor es compatible con ENERGY STAR, seleccione **Energía**; de lo contrario, seleccione **Pantalla**.
   - Si se configura el modo en **Energy (Energía)**, el artefacto deja el monitor en modo de suspensión. Por lo general, para indicar esto el monitor se apaga y una luz de color ámbar reemplaza al LED de alimentación de color verde.
   - Si se configura el modo en **Screen (Pantalla)**, el indicador de OSCAR se desplaza por toda la pantalla mientras dure la prueba. Antes de comenzar la prueba, aparece un mensaje de advertencia emergente que indica: "Energy mode may damage a monitor that is not ENERGY STAR compliant. However, once started, the test can be quit immediately via mouse or keyboard interaction." (El modo Energía puede dañar los monitores que no cumplan con ENERGY STAR. No obstante, una vez comenzada la prueba, es posible cerrarla de inmediato mediante el teclado o el mouse).

   PRECAUCIÓN: Si se utiliza el modo de Energía en monitores no compatibles con Energy Star, estos pueden sufrir daños.
5. Opcional: Para activar la prueba de protector de pantalla, haga clic en **Test (Prueba)**. Aparecerá el cuadro de diálogo **Screen Saver Test (Prueba de protector de pantalla)**. Haga clic en **OK (Aceptar)** para iniciar la prueba.
   La prueba dura 10 segundos. Al finalizar, se regresa al cuadro de diálogo **Security (Seguridad)**.

Configuración de la desconexión automática

Puede configurar OSCAR para que se desconecte automáticamente de un servidor después de un período de inactividad.

1. En el cuadro de diálogo **Principal**, haga clic en **Configuración** y después en **Seguridad**.
2. En el campo **Tiempo de inactividad**, introduzca la cantidad de tiempo que desea permanecer conectado a un servidor antes de que se produzca la desconexión automática.
3. Haga clic en **OK** (Aceptar).

Eliminación de la protección por contraseña de la consola

Para eliminar la protección por contraseña de la consola:

1. En el cuadro de diálogo **Main (Principal)**, haga clic en **Setup (Configuración)** y después en **Security (Seguridad)**.
2. En el cuadro de diálogo **Seguridad**, haga clic una vez y presione <Intro> o haga clic dos veces en el campo **Nueva**.
3. Deje en blanco el campo **Nueva** y presione <Intro>.
4. Haga clic una vez y presione <Intro> o haga doble clic en el campo **Repetir**.
5. Deje en blanco el campo **Repetir** y presione <Intro>.
6. Haga clic en **OK** (Aceptar).

Activación del modo de protector de pantalla sin contraseña

NOTA: Si su consola está protegida con contraseña, primero debe eliminar la protección por contraseña. Elimine la contraseña antes de activar el modo de protector de pantalla sin protección por contraseña.

Para activar el modo de protector de pantalla sin contraseña:

1. Seleccione **Activar protector de pantalla**.
2. Escriba la cantidad de minutos (de 1 a 99) que desea retrasar la activación del protector de pantalla.
3. Seleccione **Energía** si el monitor es compatible con ENERGY STAR; de lo contrario, seleccione **Pantalla**.

   PRECAUCIÓN: Si se utiliza el modo de Energía en monitores no compatibles con Energy Star, estos pueden sufrir daños.

4. Opcional: Para activar la prueba de protector de pantalla, haga clic en **Test (Prueba)**. Aparecerá el cuadro de diálogo **Screen Saver Test (Prueba de protector de pantalla)**. Haga clic en **OK (Aceptar)** para iniciar la prueba.

   La prueba dura 10 segundos. Una vez que se completa, aparece el cuadro de diálogo **Security (Seguridad)**.

   NOTA: Al activar el modo **Screen Saver (Protector de pantalla)** se desconecta al usuario de un servidor. Esto significa que no queda seleccionado ningún servidor. El indicador de estado señala **Free (Libre)**.

Salida del modo de protector de pantalla

Para salir del modo de protector de pantalla y regresar al cuadro de diálogo **Principal**, presione cualquier tecla o mueva el mouse.

Para apagar el protector de pantalla, en el cuadro de diálogo **Seguridad**, anule la selección del cuadro **Activar protector de pantalla** y haga clic en **Aceptar**.

Para activar el protector de pantalla de inmediato, presione <Impr Pant> y después <Pausa>.

Eliminación de una contraseña perdida u olvidada

Si pierde u olvida la contraseña del iKVM, puede restablecer la predeterminada de fábrica y luego definir una nueva. Puede restablecer la contraseña mediante la interfaz web de la CMC o RACADM.

Para restablecer una contraseña perdida u olvidada del iKVM mediante la interfaz web del CMC, en el árbol del sistema, vaya a **Descripción general del chasis** > **iKVM**, haga clic en la ficha **Configuración** y, a continuación, en **Restaurar valores predeterminados**.

Puede cambiar la contraseña predeterminada mediante OSCAR. Para obtener más información, consulte Configuración de la contraseña.

Para restablecer una contraseña perdida u olvidada con RACADM, abra una consola de texto serie/SSH/Telnet en el CMC, inicie sesión y escriba:

```
racadm racresetcfg -m kvm
```

NOTA: El comando `racresetcfg` restablece los valores de Front Panel Enable (Activación del panel frontal) y Dell CMC Console Enable (Activación de Dell CMC Console), si difieren de los valores predeterminados.

Para obtener más información acerca del subcomando `racresetcfg`, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Cambio de idioma

Utilice el cuadro de diálogo **Language (Idioma)** para elegir alguno de los idiomas ofrecidos para el texto de OSCAR. El texto se cambia inmediatamente al idioma seleccionado en todas las pantallas de OSCAR.

Para cambiar el idioma de OSCAR:

1. Presione <Impr Pant>.
   Aparecerá el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración** y después en **Idioma**.
   Aparecerá el cuadro de diálogo **Idioma**.
3. Seleccione el idioma correspondiente y haga clic en **Aceptar**.

Visualización de la información de la versión

Use el cuadro de diálogo **Versión** para ver las versiones de firmware y hardware del iKVM e identificar la configuración de idioma y teclado.

Para ver la información de la versión:

1. Presione <Impr Pant>.
   Se muestra el cuadro de diálogo **Principal**.
2. Haga clic en **Comandos** y después en **Mostrar versiones**.
   Se mostrará el cuadro de diálogo **Version (Versión)**. En la mitad superior del cuadro de diálogo **Version (Versión)** se presentan las versiones de los subsistemas.
3. Haga clic en la  o presione <Esc> para cerrar el cuadro de diálogo **Version (Versión)**.

Exploración del sistema

En el modo de exploración, el iKVM explora automáticamente cada ranura (en cada servidor). Puede explorar hasta 16 servidores, y especificar cuáles desea explorar y la cantidad de segundos que se mostrará cada uno.

Tareas relacionadas

Incorporación de servidores a la lista de exploración: en la página 206
Eliminación de un servidor de la lista de exploración en la página 207
Inicio del modo de exploración en la página 207
Cancelación del modo de exploración en la página 207

Incorporación de servidores a la lista de exploración:

Para agregar servidores a la lista de exploración:

1. Presione <Impr Pant>.
   Aparecerá el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración** y después en **Explorar**.
   Aparecerá el cuadro de diálogo **Explorar**, con la lista de todos los servidores del chasis.
3. Realice una de las siguientes acciones:
   - Seleccione los servidores que desea explorar.
   - Haga doble clic en el nombre del servidor o en la ranura.
   - Presione <Alt> y el número de servidores que desea explorar. Puede seleccionar hasta 16 servidores.
4. En el campo **Tiempo**, introduzca la cantidad de segundos (de 3 a 99) que el iKVM debe esperar antes de avanzar al siguiente servidor de la secuencia de exploración.
5. Haga clic en **Agregar/quitar** y después en **Aceptar**.

Eliminación de un servidor de la lista de exploración

Para eliminar un servidor de la lista de exploración:

1. En el cuadro de diálogo **Explorar**, realice una de las siguientes acciones:
   - Seleccione el servidor que desea quitar.
   - Haga doble clic en el nombre del servidor o en la ranura.
   - Haga clic en **Borrar** para quitar todos los servidores de la lista **Explorar**.
2. Haga clic en **Agregar/quitar** y después en **Aceptar**.

Inicio del modo de exploración

Para iniciar el modo de exploración:

1. Presione <Impr Pant>.
   Se muestra el cuadro de diálogo **Principal**.
2. Haga clic en **Comandos**.
   Se muestra el cuadro de diálogo **Comandos**.
3. Seleccione la casilla **Activar exploración**.
4. Haga clic en **OK** (Aceptar).
   Aparecerá un mensaje para indicar que el mouse y el teclado fueron restablecidos.
5. Haga clic en  para cerrar el cuadro de mensaje.

Cancelación del modo de exploración

Para cancelar el modo de exploración:

1. Si OSCAR está abierto y se muestra el cuadro de diálogo **Principal**, seleccione un servidor de la lista.

   o

   `Si OSCAR no está abierto, mueva el mouse o presione cualquier tecla.`

   Se muestra el cuadro de diálogo **Principal**. Seleccione un servidor de la lista.
2. Haga clic en **Comandos**.
   Aparecerá el cuadro de diálogo **Comandos**.
3. Desactive la opción **Activar exploración** y haga clic en **Aceptar**.

Transmisión a servidores

Puede controlar en simultáneo más de un servidor del sistema para asegurarse de que todos los servidores seleccionados reciban señales de entrada idénticas. Puede optar por transmitir pulsaciones de teclas y movimientos de mouse por separado.

- Transmisión de pulsaciones de teclas: Si utiliza pulsaciones de teclas, el estado del teclado debe ser idéntico en todos los servidores que reciben la transmisión para que la interpretación de las pulsaciones sea idéntica. Concretamente, los modos <Bloq Mayús> y <Bloq Num> deben ser iguales en todos los teclados. Mientras el iKVM intenta enviar pulsaciones de teclas a los servidores seleccionados en simultáneo, algunos servidores pueden inhibir y por ende retrasar la transmisión
- Transmisión de movimientos de mouse: Para que el mouse funcione correctamente, todos los servidores deben tener idénticos controladores de mouse, pantallas de escritorio (por ejemplo, iconos colocados en lugares idénticos) y resoluciones de video. El mouse también debe estar exactamente en el mismo lugar en todas las pantallas. Debido a que es muy difícil cumplir con estas condiciones, la transmisión de movimientos de mouse a varios servidores puede producir resultados impredecibles.

NOTA: Puede transmitir a un máximo de 16 servidores a la vez.

Para realizar la transmisión a los servidores:

1. Presione <Impr Pant>.
   Se muestra el cuadro de diálogo **Principal**.
2. Haga clic en **Configuración** y después en **Transmisión**.
   Se muestra el cuadro de diálogo **Transmisión**.
3. Para activar el mouse o el teclado de los servidores que recibirán los comandos de transmisión, seleccione las casillas.

o

Presione las flechas hacia arriba o abajo para desplazar el cursor a un servidor de destino. A continuación, presione <Alt> <K> para seleccionar la casilla del teclado o <Alt> <M> para seleccionar la del mouse. Repita este procedimiento con los servidores adicionales.

4. Haga clic en **Aceptar** para guardar los valores y regresar al cuadro de diálogo **Configuración**.
5. Haga clic en la  o presione <Esc> para regresar al cuadro de diálogo **Main (Principal)**.
6. Haga clic en **Comandos**.
   Aparecerá el cuadro de diálogo **Comandos**.
7. Haga clic en la casilla **Activar transmisión** para activarla.
   Se muestra el cuadro de diálogo **Advertencia de transmisión**.
8. Haga clic en **OK (Aceptar)** para activar la transmisión. Para cancelar y regresar al cuadro de diálogo **Commands (Comandos)**, haga clic en la  o pulse <Esc>
9. Si la transmisión está activada, escriba la información o ejecute los movimientos del mouse que desee transmitir desde la estación de administración. Solo se podrá acceder a los servidores de la lista.

Admin del iKVM desde el CMC

Puede hacer lo siguiente:

- Ver el estado y las propiedades del iKVM
- Actualizar el firmware del iKVM
- Activar o desactivar el acceso al iKVM desde el panel frontal
- Activar o desactivar el acceso al iKVM desde la consola Dell CMC

Conceptos relacionados

Actualización de firmware del iKVM en la página 48
Activación o desactivación del acceso al iKVM desde el panel frontal en la página 208

Tareas relacionadas

Visualización de información y estado de condición del iKVM en la página 73
Activación del acceso al iKVM desde Dell CMC Console en la página 209

Activación o desactivación del acceso al iKVM desde el panel frontal

Puede activar o desactivar el acceso al iKVM desde el panel frontal a través de la interfaz web del CMC o del comando RACADM.

Activación o desactivación del acceso al iKVM desde el panel frontal mediante la interfaz web

Para activar o desactivar el acceso al iKVM desde el panel frontal mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** > **iKVM** y haga clic en la ficha **Configuración**.
   Aparecerá la página **Configuración de iKVM**.
2. Para activar, seleccione la opción **Front Panel USB/Video Enabled (USB/Video del panel frontal activado)**. Para desactivar, desmarque la opción **Front Panel USB/Video Enabled (USB/Video del panel frontal activado)**.
3. Haga clic en **Aplicar** para guardar la configuración.

Activación o desactivación del acceso al iKVM desde el panel frontal con un comando de RACADM

Para activar o desactivar el acceso al iKVM desde el panel frontal con un comando de RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <value>
```

donde <value> es 1 (activar) o 0 (desactivar). Para obtener más información sobre el

```
config
```

subcomando, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Activación del acceso al iKVM desde Dell CMC Console

Para permitir el acceso a la CLI de la CMC desde iKVM mediante la interfaz web de la CMC, en el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** > **iKVM** y luego haga clic en la ficha **Setup (Configuración)**. Seleccione la opción **Allow access to CMC CLI from iKVM (Permitir acceso a la CLI de la CMC desde iKVM)** y haga clic en **Apply (Aplicar)** para guardar la configuración.

Para permitir el acceso a la CLI del CMC desde iKVM mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

Tareas relacionadas

Antes de iniciar sesión en el CMC mediante una consola serie, Telnet o SSH en la página 41

15

Admin y supervisión de la alimentación

El gabinete del servidor Dell PowerEdge M1000e es el gabinete de servidor modular con el consumo de energía más eficiente. 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 está vinculado a las capacidades sofisticadas de administración de energía incorporadas en el controlador de gestión del chasis (CMC), los suministros de energía y la iDRAC para permitirle mejorar aún más la eficiencia en el uso de la energía y para ofrecerle un control total sobre su entorno de alimentación.

Las funciones de administración de la alimentación del servidor M1000e permiten a los administradores configurar el gabinete de modo tal que se reduzca el consumo de alimentación y se ajuste la alimentación según lo requiera el entorno específico.

El gabinete modular de PowerEdge M1000e consume energía y distribuye la carga en todas las fuentes de alimentación (PSU) internas activas. El sistema puede proporcionar hasta 16685 vatios de alimentación de entrada asignada a los módulos de servidor y a la infraestructura de gabinete asociada.

El gabinete PowerEdge M1000e 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 energía a través de **Dell OpenManage Power Center**. Cuando **Dell OpenManage Power Center** controla la alimentación externamente, el CMC continúa manteniendo lo siguiente:

- Política de redundancia
- Registro remoto de la alimentación
- Rendimiento del sistema sobre redundancia de alimentación
- Conexión dinámica de suministros de energía (DPSE)
- Operación a 110 VCA. Esto solo se admite en unidades de suministro de energía de CA.

Centro de alimentación de Dell OpenManage administra:

- Alimentación del servidor
- Prioridad de los servidores
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

NOTA: La entrega real de alimentación se basa en la configuración y en la carga de trabajo.

Puede utilizar la interfaz web y RACADM para administrar y configurar los controles de alimentación en el CMC:

- Ver las asignaciones, el consumo y el estado de alimentación del chasis, de los servidores y de las unidades de suministro de energía.
- Configurar el presupuesto de alimentación y la política de redundancia del chasis.
- Ejecutar operaciones de control de alimentación (encendido, apagado, restablecimiento del sistema, ciclo de encendido) en el chasis.

Conceptos relacionados

Políticas de redundancia en la página 211
Conexión dinámica de suministros de energía en la página 214
Configuración predeterminada de redundancia en la página 215
Presupuesto de alimentación para módulos de hardware en la página 216
Visualización del estado del consumo de alimentación en la página 218
Visualización del estado del presupuesto de alimentación en la página 218
Estado de redundancia y condición general de la alimentación en la página 219
Configuración de la redundancia y el presupuesto de alimentación en la página 223
Ejecución de las operaciones de control de alimentación en la página 227

Temas:

- Conexión dinámica de suministros de energía
- Configuración predeterminada de redundancia
- Presupuesto de alimentación para módulos de hardware
- Configuración de la prioridad de alimentación de ranura del servidor
- Visualización del estado del consumo de alimentación
- Visualización del estado del presupuesto de alimentación
- Estado de redundancia y condición general de la alimentación
- Configuración de la redundancia y el presupuesto de alimentación
- Ejecución de las operaciones de control de alimentación

Políticas de redundancia

La política de redundancia es un conjunto configurable de propiedades que determina la forma en que la CMC administra la alimentación del chasis. Las siguientes políticas de redundancia son configurables con o sin conexión dinámica de unidades de suministro de energía:

- Redundancia de cuadrícula
- Redundancia del suministro de energía
- No redundancia

Política de redundancia de la red eléctrica

El objetivo de la política de redundancia de la red eléctrica es que un sistema de gabinete modular funcione en un modo que le permita tolerar fallas de alimentación. Estas fallas pueden originarse en la red eléctrica de entrada, el cableado, el suministro o en la propia unidad de suministro de energía (PSU).

Cuando se configura un sistema para la redundancia de la red eléctrica, las PSU se dividen en diferentes redes: las PSU de las ranuras 1, 2 y 3 se encuentran en la primera red, en tanto que las PSU de las ranuras 4, 5 y 6 se encuentran en la segunda red. La CMC administra la alimentación de forma tal que, si se produce una falla en alguna de las redes eléctricas, el sistema seguirá funcionando sin que haya degradación. La redundancia de la red eléctrica también tolera las fallas de PSU individuales.

NOTA: Esta redundancia ofrece operación impecable del servidor aunque falle toda una red eléctrica. Por ende, la alimentación máxima está disponible para mantener la redundancia cuando las capacidades de las dos redes son aproximadamente iguales.

NOTA: La redundancia de la red eléctrica solo se cumple cuando los requisitos de carga no superan la capacidad de la red eléctrica más débil.

Niveles de redundancia de la red eléctrica

Para configurar la redundancia de la red eléctrica, se necesita al menos una unidad de suministro de energía (PSU) presente en cada red eléctrica. Es posible definir configuraciones adicionales con cada combinación que contenga al menos una PSU en cada red eléctrica. Sin embargo, para que el máximo nivel de energía esté disponible para su uso, la energía total de las PSU de cada red eléctrica debe ser lo más similar posible. El límite máximo de energía mientras se mantiene la redundancia de la red eléctrica es la energía disponible en la red eléctrica más débil de las dos. En la siguiente figura se muestran dos PSU por cada red eléctrica y una falla de alimentación en la red eléctrica 1.

Si el CMC no puede conservar la redundancia de la red eléctrica, se envían alertas por correo electrónico o SNMP a los administradores en caso de que el suceso de **Redundancia perdida** esté configurado como alerta.

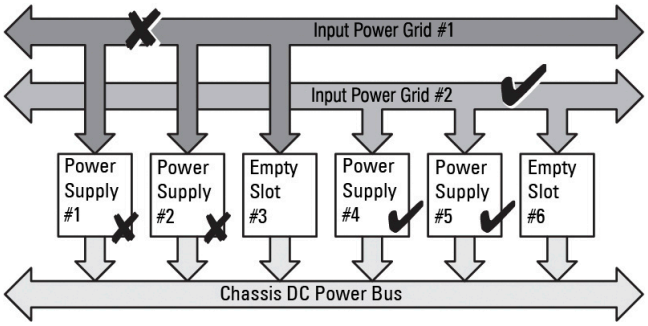


Ilustración 14. Unidades de suministro de energía por cada red eléctrica y una falla de alimentación en la red eléctrica 1

En caso de que falle una sola PSU en esta configuración, las demás PSU de la red que falle se marcarán como Online (En línea). En ese estado, las PSU de la red redundante, si no fallaron, ayudan con el funcionamiento del sistema sin interrupción. Si una PSU falla, la condición del chasis se marca como Non-Critical (No crítica). Si la red eléctrica más pequeña no puede admitir todas las asignaciones de energía del chasis, se informa que el estado de redundancia de la red eléctrica es **No Redundancy (Sin redundancia)** y la condición del chasis es **Critical (Crítica)**.

Política de redundancia de suministro de energía

La política de redundancia de suministro de energía es útil cuando las redes de energía redundante no están disponibles, pero es posible que desee estar protegido contra una falla de una única unidad de suministro de energía que deje fuera de servicio a los servidores en un gabinete modular. La unidad de suministro de energía de mayor capacidad se mantiene en reserva en línea para este propósito. Esto forma un grupo de redundancia de suministro de energía. En la figura a continuación se ilustra el modo de redundancia de suministro de energía.

Las demás unidades de suministro de energía además de las necesarias para alimentación y redundancia siguen disponibles y se agregan al grupo en caso de falla.

A diferencia de la redundancia de la red eléctrica, cuando se selecciona la redundancia de suministro de energía, CMC no requiere que las unidades de suministro de energía estén presentes en ninguna posición específica de las ranuras de las unidades de suministro de energía.

NOTA: La conexión dinámica de suministros de energía (DPSE) permite poner en espera las PSU. En espera es un estado físico durante el cual no se suministra alimentación desde la PSU. Al activar la DPSE, las PSU adicionales pueden quedar En espera para aumentar la eficiencia y ahorrar energía.

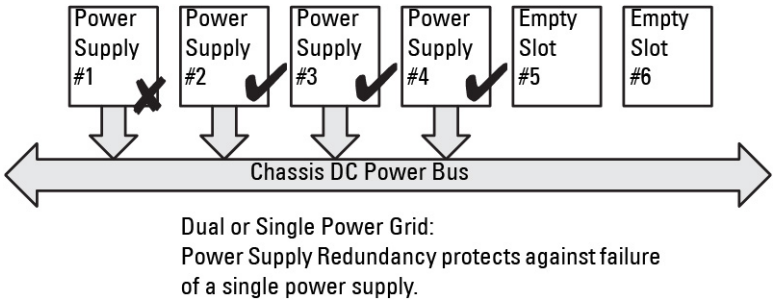


Ilustración 15. Redundancia de suministro de energía: total de 4 unidades de suministro de energía con la falla de una unidad

Sin política de redundancia

El modo sin redundancia es el valor predeterminado de fábrica para la configuración de tres unidades de suministro de energía (PSU), e indica que el chasis no tiene configurada ninguna redundancia de alimentación. En esta configuración, el estado de redundancia general del chasis indica siempre Sin redundancia. En la siguiente figura se muestra que el modo sin redundancia es el valor predeterminado de fábrica para la configuración de tres PSU.

El CMC no requiere que las unidades de suministro de energía estén presentes en una posición específica de las ranuras cuando está configurado el modo **Sin redundancia**.

NOTA: Todas las PSU del chasis están **En línea** si la DPSE está desactivada con el modo **Sin redundancia**. Cuando se activa la DPSE, todas las PSU activas del chasis aparecen como **En línea** y las PSU adicionales pueden quedar **En espera** para aumentar la eficiencia energética del sistema.

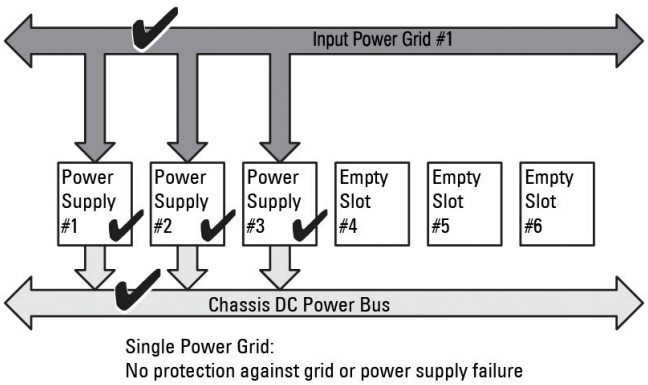


Ilustración 16. Sin redundancia con tres unidades de suministro de energía en el chasis

Una falla en una PSU hace que las demás salgan del modo En espera, según sea necesario, para cubrir las asignaciones de energía del chasis. Si existen cuatro PSU y solo se requieren tres, en el caso de que una falle, la cuarta unidad se pone en línea. Un chasis puede tener las seis PSU en línea.

Al activar la DPSE, las PSU adicionales pueden quedar En espera para aumentar la eficiencia y ahorrar energía. Para obtener más información, consulte Configuración predeterminada de redundancia.

Rendimiento de alimentación extendida

El modo Rendimiento de alimentación extendida (EPP) permite asignar, en una configuración de seis unidades de suministro de energía (PSU), para el chasis M1000e, un 30% más de alimentación que la alimentación redundante en una configuración de redundancia de la red eléctrica con varias PSU de 3000 W de CA. Sin embargo, la alimentación asignada a los servidores se reduce automáticamente en el caso de que se produzca una falla en la red de CA o en la PSU, con el fin de que los servidores no se apaguen. Se puede asignar un máximo de 2700 W de alimentación para los chasis con configuraciones superiores.

De manera predeterminada, la función EPP se encuentra activada en la configuración de seis suministros de energía de 3000 W de CA. Puede ver la configuración actual, desactivar y activar esta función en la interfaz web y en la interfaz de línea de comandos.

La función EPP permite las asignaciones de alimentación solamente cuando:

- Se ha configurado la alimentación para Redundancia de la red eléctrica.
- Existen seis unidades de suministro de energía de tipo 3000 W de CA.
- El valor de Límite de alimentación de entrada del sistema es mayor que 13300 W de CA (45381 BTU/h).

La alimentación ganada mediante el modo EPP está disponible para mejorar el rendimiento de los servidores. Cuando se compara con una configuración de seis PSU de 2700 W de CA, la alimentación adicional obtenida en una configuración de seis PSU de 3000 W de CA con el modo de refrigeración mejorado para ventiladores habilitado y activado es de 723 W. Cuando se compara con una configuración de seis PSU de 2700 W de CA, la alimentación adicional obtenida en el modo de configuración de ventiladores estándar es de 1023 W.

La alimentación adicional disponible de EPP es 2700 W, que se pueden usar solamente para aumentar el rendimiento de los servidores.

El modo EPP se puede activar únicamente cuando las siguientes funciones de alimentación se encuentran desactivadas:

- Modo de conservación máx. de alimentación (MPCM)
- Conexión dinámica de suministros de energía (DPSE)
- Administración de la alimentación basada en servidor (SBPM)
- Rendimiento de servidor sobre redundancia de alimentación (SPOPR)

Si se intenta activar EPP cuando cualquiera de las funciones MPCM, DPSE, SBPM o SPOPR se encuentra activada, aparece un mensaje. En el mensaje, se solicita desactivar estas cuatro funciones para poder activar el modo Rendimiento de alimentación extendida. Cuando se activa el modo, ninguna de las funciones DPSE, SBPM y SPOPR puede estar activada. Se le solicitará que desactive la función Rendimiento de alimentación extendida para poder activar cualquiera de estas tres funciones.

Cuando el chasis está equipado con PSU de 3000 W de CA, el firmware actual bloquea los intentos de volver a versiones anteriores a CMC 4.5. Esto se debe a que las versiones del firmware de la CMC anteriores a la 4.5 no admiten PSU de 3000 W de CA.

Opciones de configuración de la alimentación predeterminadas con rendimiento de alimentación extendida

Opciones de configuración de la alimentación predeterminadas en el chasis cuando el modo EPP se encuentra activado o desactivado:

- En una configuración de seis unidades de suministro de energía de 3000 W de CA con la política Redundancia de la red eléctrica:

  EPP Activado – DPSE Desactivado, SPOPR Desactivado, MPCM Desactivado, SBPM Desactivado

- Al ejecutar el comando `racadm racresetcfg` en una configuración de unidad de suministro de energía de 3000 W de CA, se restablece la configuración de la alimentación a los siguientes valores:

  EPP Desactivado – DPSE Desactivado, SPOPR Desactivado, MPCM Desactivado, SBPM Desactivado

- En una configuración de menos de seis unidades de suministro de energía de 3000 W de CA:

  EPP Desactivado – DPSE Desactivado, SPOPR Desactivado, MPCM Desactivado, SBPM Desactivado

- En una configuración de unidad de suministro de energía de 2700 W de CA:

  EPP Desactivado – DPSE Desactivado, SPOPR Activado, MPCM Desactivado, SBPM Desactivado

- Al usar el comando racadm racresetcfg en una configuración de unidad de suministro de energía de 2700 W de CA, se restablece la configuración de la alimentación a los siguientes valores:

  EPP Desactivado – DPSE Desactivado, SPOPR Desactivado, MPCM Desactivado, SBPM Desactivado

- En una configuración de chasis con la opción Fresh Air activada, las unidades de suministro de energía de 3000 W se muestran como de 2800 W y EPP no es compatible.

Conexión dinámica de suministros de energía

El modo Conexión dinámica de suministros de energía (DPSE) está desactivado de manera predeterminada. La DPSE ahorra energía al optimizar la eficiencia de consumo proporcionada por las unidades de suministro de energía (PSU) del chasis. Esto también alarga la vida útil de las PSU y reduce la generación de calor.

La CMC supervisa la asignación de alimentación total del gabinete y lleva las PSU al estado En espera. Al llevar las PSU al estado En espera:

- Se permite la entrega de la asignación total de alimentación del chasis a través de menos PSU.
- Mejora la eficiencia de las PSU en línea, ya que funcionan con una utilización mayor.
- Aumenta la eficiencia y la durabilidad de las PSU en espera.

Para que las unidades de suministro de energía restantes funcionen con máxima eficiencia:

- El modo **Sin redundancia** con DPSE ofrece gran eficiencia energética, con una cantidad óptima de PSU en línea. Las PSU que no se necesitan se dejan en el modo En espera.
- El modo **Redundancia de PSU** con DPSE también ofrece eficiencia energética. Por lo menos hay dos suministros en línea. Una PSU impulsa la configuración, mientras que la otra ofrece redundancia por si falla la primera. El modo Redundancia de PSU ofrece protección contra la falla de cualquier PSU, pero no ofrece protección ante una pérdida de la red eléctrica de CA.
- El modo **Redundancia de la red eléctrica** con DPSE, en el que al menos dos de los suministros están activos, uno en cada red eléctrica, proporciona un buen equilibrio entre eficiencia y disponibilidad máxima para una configuración de gabinete modular parcialmente cargado.
- La desactivación de la DPSE proporciona la más baja eficiencia ya que los seis suministros están activos y comparten la carga. Esto produce una utilización más baja de cada suministro de energía.

La DPSE puede activarse para las tres configuraciones de redundancia de suministro de energía: **Sin redundancia**, **Redundancia de suministro de energía** y **Redundancia de la red eléctrica**.

- En una configuración **Sin redundancia** con DPSE, el M1000e puede tener hasta cinco unidades de suministro de energía en estado **En espera**. En una configuración de seis PSU, algunas se dejarán **En espera** y no se utilizarán para mejorar la eficiencia energética. La eliminación o falla de una PSU en línea en esta configuración ocasiona que una PSU **En espera** pase a quedar **En línea**. Sin embargo, las PSU en espera pueden tardar hasta 2 segundos en activarse, de manera que algunos módulos de servidor pueden perder alimentación durante la transición en la configuración **Sin redundancia**.

  NOTA: En una configuración de tres unidades de suministro de energía, la carga del servidor puede impedir que una unidad de suministro de energía haga la transición a En espera.

- En una configuración de **Redundancia del suministro de energía**, el gabinete siempre mantiene una PSU adicional encendida y marcada como **En línea**, además de las PSU necesarias para encender el gabinete. El uso de alimentación se supervisa, y hasta cuatro PSU pueden quedar En espera según la carga general del sistema. En una configuración de seis PSU, por lo menos dos unidades de suministro de energía se encuentran siempre encendidas.

  Dado que un gabinete en la configuración de **Redundancia del suministro de energía** siempre tiene una PSU adicional conectada, el gabinete puede tolerar la pérdida de una PSU en línea. Además, así el gabinete puede tener suficiente energía para los módulos de

servidor instalados. La pérdida de la PSU en línea hará que una PSU en espera pase a estar en línea. La falla simultánea de varias PSU puede ocasionar la pérdida de energía en algunos módulos de servidor mientras las PSU en espera se encienden.

- En la configuración de **Redundancia de la red eléctrica**, todos los suministros de energía están conectados cuando el chasis está encendido. Se supervisa la utilización de energía y, si la configuración del sistema y la utilización de energía lo permiten, las PSU quedan **En espera**. El estado **En línea** de las PSU en una red eléctrica refleja el de la otra red eléctrica. En consecuencia, se puede soportar la pérdida de energía de toda una red sin interrumpir el suministro de energía al gabinete.

  Un aumento de la demanda de energía en la configuración de **Redundancia de la red eléctrica** hará que las PSU se conecten y salgan del estado **En espera**. Esto mantiene la configuración duplicada necesaria para la redundancia de doble red eléctrica.

  NOTA: Con la DPSE activada, las unidades de suministro de energía en espera se ponen **En línea** para recuperar energía si la demanda aumenta en los tres modos de la política de redundancia de alimentación.

Configuración predeterminada de redundancia

La configuración predeterminada de redundancia para un chasis depende del número de unidades de suministro de energía que contiene, como se muestra en la siguiente tabla.

Tabla 44. Configuración predeterminada de redundancia

Configuración de unidades de suministro de energía	Política de redundancia predeterminada	Valor predeterminado de la conexión dinámica de unidades de suministro de energía
Seis unidades de suministro de energía	Redundancia de cuadrícula	Desactivado
Tres unidades de suministro de energía	No redundancia	Desactivado

Redundancia de cuadrícula

En el modo de redundancia de la red eléctrica con seis unidades de suministro de energía (PSU), las seis PSU están activas. Las tres PSU de la izquierda deben estar conectadas a una red eléctrica de entrada, mientras que las tres PSU de la derecha deben estar conectadas a otra red eléctrica.

PRECAUCIÓN: Para evitar una falla del sistema y para que la redundancia de la red eléctrica funcione de manera eficaz, debe haber un conjunto equilibrado de unidades de suministro de energía correctamente cableadas a redes independientes.

Si una red eléctrica falla, las unidades de suministro de energía de la red en funcionamiento tomarán el control sin interrupción para los servidores o la infraestructura.

PRECAUCIÓN: En el modo de redundancia de la red eléctrica, debe tener dos conjuntos equilibrados de PSU (al menos una PSU en cada red eléctrica). Si esta condición no se cumple, la redundancia de la red eléctrica quizás no sea posible.

Redundancia del suministro de energía

Cuando se activa la redundancia de suministro de energía, una de las unidades de suministro de energía (PSU) del chasis se mantiene como repuesto, lo cual garantiza que la falla de una de las PSU no ocasione que se apaguen los servidores ni el chasis. El modo de redundancia de suministro de energía requiere hasta cuatro PSU. Si existen PSU adicionales, se utilizan para mejorar la eficiencia energética del sistema cuando la DPSE está activada. Las fallas posteriores a una pérdida de redundancia pueden provocar que los servidores del chasis se apaguen.

No redundancia

Hay más alimentación de la que es necesaria para alimentar el chasis, incluso en caso de falla.

PRECAUCIÓN: En el modo sin redundancia se utiliza un número óptimo de unidades de suministro de energía (PSU) cuando la DPSE se activa por los requisitos del chasis. Con este modo, la falla de una sola PSU podría provocar la pérdida de energía y datos en los servidores.

Presupuesto de alimentación para módulos de hardware

El CMC ofrece un servicio de presupuesto de alimentación que le permite configurar el presupuesto de alimentación, la redundancia y la alimentación dinámica para el chasis.

El servicio de administración de la alimentación permite optimizar el consumo de alimentación y reasignar la alimentación a diferentes módulos en función de la demanda.

En la siguiente figura se muestra un chasis con una configuración de seis unidades de suministro de energía. Las unidades llevan del número 1 al 6 contando desde la izquierda del gabinete.

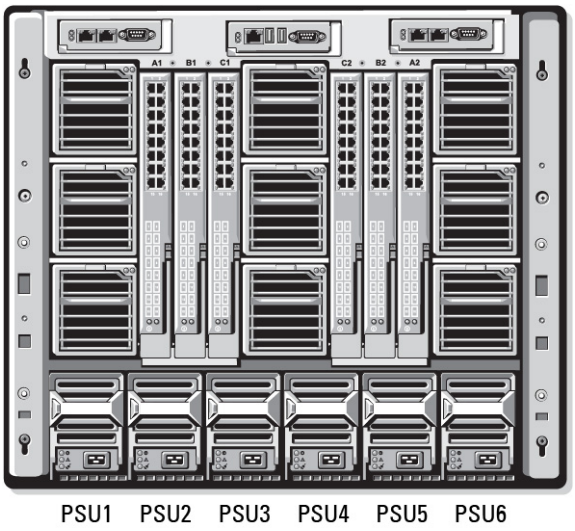


Ilustración 17. Configuración de chasis con seis unidades de suministro de energía

El CMC mantiene un presupuesto de alimentación para el gabinete que reserva la potencia necesaria para todos los servidores y componentes instalados.

La CMC asigna la alimentación a la infraestructura de la CMC y los servidores del chasis. La infraestructura de la CMC consta de los componentes dentro del chasis, como ventiladores, módulos de E/S o iKVM (de existir). El chasis puede tener hasta 16 servidores que se comunican con el chasis mediante la iDRAC. Para obtener más información, consulte la publicación *iDRAC User's Guide (Guía del usuario de iDRAC)* en **support.dell.com/manuals**.

La iDRAC brinda los requisitos de envolvente de potencia de la CMC antes de encender el servidor. La envolvente de potencia consiste en los requisitos máximo y mínimo de alimentación para mantener el servidor en funcionamiento. El cálculo inicial de la iDRAC se basa en la interpretación inicial de los componentes del servidor. Después de iniciar el funcionamiento y detectar otros componentes, la iDRAC puede aumentar o reducir sus requisitos de alimentación iniciales.

Cuando se enciende un servidor en un gabinete, el software del iDRAC vuelve a calcular los requisitos de alimentación y solicita el cambio correspondiente en la envolvente de potencia.

La CMC otorga la alimentación solicitada al servidor, y la potencia asignada se resta del presupuesto disponible. Una vez que el servidor obtiene la alimentación solicitada, el software de la iDRAC del servidor supervisa continuamente el consumo de alimentación real. Según los requerimientos reales de alimentación, la envolvente de potencia de la iDRAC puede modificarse con el paso del tiempo. La iDRAC solicita más alimentación solamente cuando los servidores están consumiendo toda la alimentación asignada.

En condiciones de carga pesada, el funcionamiento de los procesadores del servidor puede degradarse para garantizar que el consumo de alimentación se mantenga por debajo del valor de *Límite de alimentación de entrada del sistema* configurado por el usuario.

El gabinete PowerEdge M1000e puede suministrar suficiente alimentación para el rendimiento máximo de la mayoría de las configuraciones de servidor, pero muchas de las configuraciones disponibles no consumen la alimentación máxima que el gabinete puede suministrar. Para ayudar a los centros de datos a aprovisionar alimentación para sus gabinetes, el M1000e le permite especificar un *límite de alimentación de entrada del sistema*, para asegurarse de que el consumo global de corriente alterna del chasis permanezca por debajo de un umbral determinado. La CMC primero garantiza que haya suficiente alimentación disponible para que funcionen los ventiladores, los módulos de E/S, iKVM (de existir) y la propia CMC. Esta asignación de energía se denomina la *alimentación de entrada asignada a la infraestructura de chasis*. Después de la infraestructura del chasis, se encienden los servidores del gabinete. Cualquier intento de establecer un *límite de alimentación de entrada del sistema* inferior al consumo real fracasará.

Si es necesario para que el presupuesto total de alimentación permanezca por debajo del valor del *límite de alimentación de entrada del sistema*, la CMC asigna los servidores un valor menor a la alimentación máxima solicitada. A los servidores se les asigna alimentación de acuerdo con su configuración de *prioridad de los servidores*: los servidores con prioridad más alta reciben el máximo de alimentación, los

servidores con prioridad 2 reciben alimentación después de los servidores con prioridad 1, y así sucesivamente. Los servidores de menor prioridad pueden recibir menos alimentación que los servidores de prioridad 1 en función de la *capacidad máxima de alimentación de entrada del sistema* y la configuración definida por el usuario del *límite de alimentación de entrada del sistema*.

Los cambios de configuración, como un servidor adicional en el chasis, pueden requerir que se aumente el *límite de alimentación de entrada del sistema*. Las necesidades energéticas en un gabinete modular aumentan también cuando cambian las condiciones térmicas y es necesario que los ventiladores funcionen a mayor velocidad, lo que provoca que consuman energía adicional. La inserción de módulos de E/S e iKVM también aumenta las necesidades de alimentación del gabinete modular. Aunque estén apagados, los servidores consumen una pequeña cantidad de energía para mantener encendida la controladora de administración.

Los servidores adicionales se pueden encender en el gabinete modular solo si hay suficiente energía disponible. El *límite de alimentación de entrada del sistema* puede aumentarse en cualquier momento hasta un valor máximo de 16685 vatios, para permitir el encendido de servidores adicionales.

Los cambios en el gabinete modular que reducen la asignación de alimentación son:

- Apagado del servidor
- Servidor
- Módulo de E/S
- Retiro del iKVM
- Transición del chasis al estado apagado

Los usuarios pueden reconfigurar el *Límite de alimentación de entrada del sistema* cuando el chasis está encendido o apagado.

Configuración de la prioridad de alimentación de ranura del servidor

La CMC le permite definir una prioridad de alimentación para cada una de las dieciséis ranuras de servidor de los gabinetes. Los valores de prioridad van de 1 (la más alta) a 9 (la más baja). Estos valores se asignan a las ranuras del chasis, y todo servidor insertado en esa ranura hereda la prioridad de la ranura. La CMC utiliza la prioridad de ranura para administrar la alimentación privilegiando a los servidores de mayor prioridad del gabinete.

Según el valor predeterminado de prioridad de las ranuras de servidor, la alimentación se distribuye por igual a todas las ranuras. Al cambiar las prioridades de las ranuras, los administradores pueden priorizar a los servidores que prefieran para las asignaciones de alimentación. Si los módulos de servidor más importantes se dejan con la prioridad de ranura predeterminada 1 y los módulos de servidor menos importantes se cambian a un valor de menor prioridad 2 o un número mayor, los módulos de servidor de prioridad 1 se encienden primero. Estos servidores de prioridad más alta obtienen su asignación máxima de alimentación, mientras que a los servidores de prioridad más baja quizás no se les asigne suficiente alimentación para tener su máximo rendimiento o quizás ni siquiera se enciendan, dependiendo de lo bajo que se haya definido el límite de alimentación de entrada del sistema y los requisitos de alimentación de los servidores.

Si un administrador enciende manualmente los módulos de servidor de baja prioridad antes que los de prioridad más alta, los de prioridad baja serán los primeros módulos a los que se les disminuya su asignación de alimentación al valor mínimo, a fin de abastecer a los servidores de mayor prioridad. Por lo tanto, cuando se agota la alimentación disponible para asignar, la CMC recupera alimentación de los servidores de prioridad inferior o similar hasta que alcancen el nivel mínimo.

NOTA: A los módulos de E/S, los ventiladores e iKVM (de existir) se les asigna la más alta prioridad. La CMC recupera alimentación solo de los dispositivos de menor prioridad para satisfacer las necesidades de alimentación de módulos o servidores de mayor prioridad.

Asignación de niveles de prioridad a los servidores

Los niveles de prioridad de servidor determinan de cuáles servidores obtiene energía el CMC cuando se necesita energía adicional.

NOTA: La prioridad que se asigna a un servidor está vinculada a la ranura y no al servidor en sí mismo. Si traslada el servidor a una nueva ranura, debe reconfigurar la prioridad para la ubicación en la nueva ranura.

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Asignación de niveles de prioridad a los servidores mediante la interfaz web del CMC

Para asignar niveles de prioridad mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Alimentación** > **Prioridad**.
   La página **Prioridad de los servidores** muestra todos los servidores del chasis.
2. Seleccione un nivel de prioridad (de 1 a 9, donde 1 es la prioridad máxima) para uno, varios o todos los servidores. El valor predeterminado es 1. Puede asignar el mismo nivel de prioridad a varios servidores.
3. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Asignación de niveles de prioridad a los servidores mediante RACADM

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

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <slot number> <priority level>
```

Donde *<número de ranura>* (de 1 a 16) se refiere a la ubicación del servidor y *<nivel de prioridad>* es un valor entre 1 y 9.

Por ejemplo, para establecer el nivel de prioridad en 1 para el servidor en la ranura 5, escriba el siguiente comando:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

Visualización del estado del consumo de alimentación

La CMC proporciona el consumo real de alimentación de entrada para todo el sistema.

Visualización del estado del consumo de alimentación mediante la interfaz web del CMC

Para ver el estado del consumo de alimentación por medio de la interfaz web de la CMC, en el árbol del sistema vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **Power (Alimentación)** > **Power Monitoring (Supervisión de alimentación)**. La página Power Monitoring (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 *CMC Online Help (Ayuda en línea para el CMC)*.

NOTA: También puede ver el estado de redundancia de alimentación en Power Supplies (Suministros de energía), en la ficha **Árbol del sistema** > **Status (Estado)**.

Visualización del estado del consumo de alimentación con el comando RACADM

Para ver el estado del consumo de alimentación con el comando RACADM:

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

```
racadm getpminfo
```

Visualización del estado del presupuesto de alimentación

Es posible ver el estado del presupuesto de alimentación mediante la interfaz web del CMC o RACADM.

Visualización del estado de presupuesto de alimentación mediante la interfaz web del CMC

Para ver el estado del presupuesto de alimentación por medio de la interfaz web de la CMC, en el árbol del sistema vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **Power (Alimentación)** > **Budget Status (Estado de presupuesto)**. La página **Power Budget Status (Estado de presupuesto de alimentación)** muestra la configuración de la política de alimentación del sistema, los detalles del presupuesto de alimentación, el presupuesto asignado a los módulos del servidor y los detalles del suministro de energía del chasis. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

Estado de redundancia y condición general de la alimentación

El estado de redundancia es un factor determinante de la condición general de la alimentación. Cuando se establece la política de redundancia de alimentación, por ejemplo, en Grid Redundancy (Redundancia de la red eléctrica), y el estado de redundancia indica que el sistema funciona con redundancia, la condición general de la alimentación normalmente será **OK (Bueno)**. Si la unidad de suministro de energía de un chasis falla debido a alguna razón, el estado de la condición general de la alimentación del chasis se muestra como **Non-Critical (No crítico)**. Sin embargo, si no se satisfacen las condiciones para operar con redundancia de la red eléctrica, el estado de redundancia será **No** y el estado de la condición general de la alimentación será **Critical (Crítico)**. Esto se debe a que el sistema no puede funcionar de acuerdo con la política de redundancia configurada.

NOTA: La CMC no realiza una comprobación previa de estas condiciones cuando la política de redundancia se cambia de o a redundancia de la red eléctrica. Por lo tanto, configurar la política de redundancia podría ocasionar inmediatamente una pérdida o recuperación de la redundancia.

Conceptos relacionados

Falla de la unidad de suministro de energía con política de redundancia Degradada o Sin redundancia en la página 219
Retiro de unidades de suministro de energía con política de redundancia Degradada o Sin redundancia. en la página 220
Política de conexión de servidores nuevos en la página 220
Cambios de suministro de energía y política de redundancia en el registro de sucesos del sistema en la página 221

Falla de la unidad de suministro de energía con política de redundancia Degradada o Sin redundancia

La CMC reduce la alimentación de los servidores cuando se produce un suceso de alimentación insuficiente, como la falla de una unidad de suministro de energía. Después de reducir la alimentación de los servidores, la CMC vuelve a evaluar las necesidades de alimentación del chasis. Si aún no se cumple con los requisitos de alimentación, la CMC apagará los servidores de menor prioridad.

La alimentación de los servidores de mayor prioridad se restablece gradualmente, en tanto que las necesidades de alimentación se ajusten al presupuesto de alimentación. Para establecer la política de redundancia, consulte Configuración de la redundancia y el presupuesto de alimentación.

NOTA: Cuando un chasis supera el presupuesto de alimentación, la CMC muestra el mensaje `Unable to turn on Module-x because of insufficient power.`.

Retiro de unidades de suministro de energía con política de redundancia Degradada o Sin redundancia.

Es posible que la CMC comience a conservar energía cuando se quita una unidad de suministro de energía (PSU) o el cable de CA de una PSU. La CMC reduce la alimentación de los servidores de menor prioridad hasta que la asignación de energía sea cubierta por las PSU restantes del chasis. Si quita más de una PSU, la CMC volverá a evaluar las necesidades de alimentación al quitar la segunda PSU a fin de determinar la respuesta del firmware. Si aún no se cumple con los requisitos de alimentación, la CMC puede apagar los servidores de menor prioridad.

Límites

- El CMC no admite el apagado *automatizado* de un servidor con menor prioridad para permitir el encendido de un servidor con mayor prioridad; sin embargo, se pueden realizar apagados iniciados por el usuario.
- Los cambios en la política de redundancia de las PSU están limitados por el número de PSU del chasis. Puede seleccionar cualquiera de los tres valores de configuración de redundancia de PSU que se presentan en Configuración predeterminada de redundancia.

Política de conexión de servidores nuevos

Si un servidor nuevo que está encendido exige más de la alimentación disponible para el chasis, es posible que la CMC disminuya la alimentación hacia los servidores de menor prioridad. Esto permite que el nuevo servidor reciba más alimentación. Esto sucede si ocurre lo siguiente:

- El administrador ha configurado un límite de alimentación para el chasis que es inferior a la alimentación requerida para una asignación de alimentación completa a los servidores.
- No existe alimentación suficiente disponible para el requisito de alimentación para el peor de los casos de todos los servidores en el chasis.

Si no se puede liberar suficiente alimentación mediante la reducción de la alimentación asignada a los servidores con menor prioridad, es posible que el nuevo servidor no se pueda encender.

La mayor cantidad de alimentación sostenida que se requiere para ejecutar el chasis y todos los servidores, incluso el nuevo, con alimentación máxima es el requisito de alimentación para el peor de los casos. Si esa alimentación está disponible, a ningún servidor se le asigna menos energía de la que se necesita para el peor de los casos, y el nuevo servidor también se podrá encender.

En la siguiente tabla se describen las acciones realizadas por el CMC cuando se enciende un nuevo servidor en las condiciones descritas anteriormente.

Tabla 45. Respuesta del CMC cuando se intenta encender un servidor

Se cuenta con alimentación para el peor de los casos	Respuesta del CMC	Encendido del servidor
Sí	No se requiere la conservación de energía	Permitido
No	Se ejecuta la conservación de energía: ● La alimentación requerida para el nuevo servidor está disponible ● La alimentación requerida para el nuevo servidor no está disponible	Permitido No permitido

Si una unidad de suministro de energía (PSU) falla, se alcanza un estado de condición no crítica y se genera un suceso de falla de PSU. Al retirar una PSU se genera un suceso de retiro de PSU.

Si uno de los sucesos ocasiona una pérdida de redundancia, en función de las asignaciones de alimentación, se genera un suceso de *pérdida de redundancia*.

Si la capacidad de alimentación posterior o la capacidad de alimentación del usuario es mayor que las asignaciones de los servidores, el rendimiento de los servidores se verá reducido o, en el peor de los casos, los servidores pueden llegar a apagarse. Ambas condiciones se dan en orden inverso al de prioridad, es decir, los servidores de menor prioridad se apagan primero.

En la siguiente tabla se describe la respuesta del firmware ante el apagado o el desmontaje de una unidad de suministro de energía conforme se aplica a diversas configuraciones de redundancia de las unidades de suministro de energía.

Tabla 46. Impacto en el chasis de la falla o el desmontaje de una unidad de suministro de energía

Configuración de unidades de suministro de energía	Acoplamiento dinámico de unidades de suministro de energía	Respuesta del firmware
Redundancia de cuadrícula	Desactivado	El CMC informa al usuario que hay pérdida de redundancia de la red eléctrica.
Redundancia del suministro de energía	Desactivado	El CMC informa al usuario que hay pérdida de redundancia de suministro de energía.
No redundancia	Desactivado	Se disminuye la alimentación en los servidores con menor prioridad en caso de ser necesario.
Redundancia de cuadrícula	Activado	El CMC informa al usuario que hay pérdida de redundancia de la red eléctrica. Las PSU en modo de espera (si hay) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el retiro de la PSU.
Redundancia del suministro de energía	Activado	El CMC informa al usuario que hay pérdida de redundancia de suministro de energía. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el desmontaje de una unidad de suministro de energía.
No redundancia	Activado	Se disminuye la alimentación en los servidores con menor prioridad en caso de ser necesario.

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

Los cambios en el estado de suministro de energía y en la política de redundancia de la alimentación se registran como sucesos. Los sucesos relacionados con el suministro de energía que ingresan entradas en el registro de sucesos del sistema (SEL) son la inserción y extracción de suministros de energía, la inserción y extracción de entradas de suministros de energía, y la declaración y el retiro de declaración de salidas de suministros de energía.

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

Tabla 47. Sucesos del SEL para cambios de suministros de energía

Suceso de suministro de energía	Anotación del registro de sucesos del sistema (SEL)
Inserción	Power supply <*number*> is present. (La fuente de alimentación <número> está presente).
Extracción	Power supply <*number*> is absent. (Falta la fuente de alimentación <número>).
Se ha perdido la redundancia de la red eléctrica o de la fuente de alimentación	Se ha perdido la redundancia de la fuente de alimentación.
Se ha vuelto a obtener la redundancia de la fuente de alimentación	The power supplies are redundant. (Las fuentes de alimentación son redundantes).
Se ha recibido alimentación de entrada	The input power for power supply <*number*> has been restored. (Se ha restaurado la alimentación de entrada de la fuente de alimentación <número>).
Se ha perdido la alimentación de entrada	The input power for power supply <*number*> has been lost. (Se ha perdido la alimentación de entrada de la fuente de alimentación <número>).
Salida de CC producida	Power supply <*number*> is operating normally. (La fuente de alimentación <número> funciona normalmente).
Salida de CC perdida	Power supply <*number*> failed. (Se ha producido un error en la fuente de alimentación <número>).
Sobrevoltaje en la entrada	An over voltage fault detected on power supply <*number*>. (Se detectó un error de exceso de voltaje en la fuente de alimentación <número>).

Tabla 47. Sucesos del SEL para cambios de suministros de energía (continuación)

Suceso de suministro de energía	Anotación del registro de sucesos del sistema (SEL)
Falta de voltaje en la entrada	An under voltage fault detected on power supply <*number*>. (Se detectó un error de falta de voltaje en la fuente de alimentación <número>).
Exceso de corriente en la entrada	An over current fault detected on power supply <*number*>. (Se detectó un error de exceso de corriente en la fuente de alimentación <número>).
Falta de corriente en la entrada	An undercurrent fault detected on power supply <*number*>. (Se detectó un error de falta de corriente en la fuente de alimentación <número>).
Falta de voltaje en la salida de CC	An output under voltage fault detected on power supply <*number*>. (Se detectó un error de falta de voltaje de salida en la fuente de alimentación <número>).
Exceso de corriente en la salida de CC	An output over current fault detected on power supply <*number*>. (Se detectó un error de exceso de corriente de salida en la fuente de alimentación <número>).
Falta de corriente en la salida de CC	An output under current fault detected on power supply <*number*>. (Se detectó un error de falta de corriente de salida en la fuente de alimentación <número>).
Falla de comunicación	Cannot communicate with power supply <*number*>. (No se puede establecer la comunicación con la fuente de alimentación <número>).
Se restableció la comunicación	Communication has been restored to power supply <*number*>. (Se ha restablecido la comunicación en la fuente de alimentación <número>).
No se pudo comunicar la información de estado	Cannot obtain status information from power supply <*number*>. (No se pudo obtener la información de estado de la fuente de alimentación <número>).
Se ha restablecido la comunicación de datos de estado	Power supply <number> status information successfully obtained. (Se ha obtenido con éxito la información de estado de la fuente de alimentación <número>).
Falta o exceso de temperatura	The temperature for power supply <*number*> is outside of range. (La temperatura de la fuente de alimentación <número> se encuentra fuera de rango).
Error/advertencia de ventilador o flujo de aire	Fan failure detected on power supply <*number*>. (Se detectó un error de ventilador en la fuente de alimentación <número>).
Velocidad del ventilador anulada	Fan failure detected on power supply <*number*>. (Se detectó un error de ventilador en la fuente de alimentación <número>).
Falla de fabricación	Power supply <*number*> failed. (Se ha producido un error en la fuente de alimentación <número>).
Microprocesador ocupado	Power supply <*number*> failed. (Se ha producido un error en la fuente de alimentación <número>).
Error de FRU	Power supply <*number*> failed. (Se ha producido un error en la fuente de alimentación <número>).
Operación a 110 V no reconocida	Se declara un bajo voltaje de entrada (110) de suministro de energía.
Operación a 110 V reconocida	Se retira la declaración de un bajo voltaje de entrada (110) de suministro de energía.

Los sucesos relacionados con cambios en el estado de redundancia de alimentación que ingresan entradas en el SEL son la pérdida de redundancia y la recuperación de redundancia para el gabinete modular que está configurado para una política de alimentación de **Redundancia de la red eléctrica** o para una política de **Redundancia de suministros de energía**. En la tabla siguiente se enumeran las anotaciones del SEL relacionadas con los cambios en la política de redundancia de alimentación.

Tabla 48. Sucesos del SEL para cambios en la política de redundancia de alimentación

Suceso de política de alimentación	Anotación del registro de sucesos del sistema (SEL)
Redundancia perdida	Se declara la pérdida de redundancia.
Redundancia recuperada	Se retira la declaración de pérdida de redundancia.

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, iKVM, CMC y suministros de energía), el cual utiliza seis unidades de suministro de energía (PSU). El servicio de administración de alimentación optimiza el consumo de energía y reasigna la alimentación eléctrica a los distintos módulos en función de los requisitos.

Puede configurar los siguientes atributos:

- Límite de alimentación de entrada del sistema
- Política de redundancia
- Rendimiento de alimentación extendida
- Rendimiento del servidor sobre redundancia de alimentación
- Conexión dinámica de suministros de energía
- Desactivar botón de encendido del chasis
- Permitir operación a 110 VCA
- Modo de conservación máx. de alimentación
- Registro remoto de la alimentación
- Intervalo del registro remoto de la alimentación
- Administración de la alimentación basada en servidor
- Desactivar restablecimiento de la alimentación de CA

Conceptos relacionados

Conservación de la energía y presupuesto de alimentación en la página 223
Modo de conservación máxima de energía en la página 223
Reducción de la alimentación del servidor para mantener el presupuesto de alimentación en la página 224
Operación de unidades de suministro de energía de 110 V en la página 224
Rendimiento del servidor sobre redundancia de alimentación en la página 224
Registro remoto en la página 224
Admin de la alimentación externa en la página 225

Tareas relacionadas

Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web del CMC en la página 225
Configuración de la redundancia y el presupuesto de alimentación mediante RACADM en la página 226

Conservación de la energía y presupuesto de alimentación

La CMC conserva la energía cuando se llega al límite de alimentación máxima configurado por el usuario. Cuando la demanda de energía supera el límite de alimentación de entrada del sistema configurado por el usuario, la CMC reduce la alimentación para los servidores en orden inverso al de prioridad. Esto permite que haya energía para los servidores de mayor prioridad y los otros módulos del chasis.

Si varias o todas las ranuras del chasis están configuradas con el mismo nivel de prioridad, la CMC disminuye la alimentación de los servidores en el orden de los números de ranura. Por ejemplo, si los servidores en las ranuras 1 y 2 tienen el mismo nivel de prioridad, la alimentación para el servidor de la ranura 1 se reduce antes que la del servidor de la ranura 2.

NOTA: Puede asignar un nivel de prioridad del 1 al 9 a cada uno de los servidores del chasis. El nivel de prioridad predeterminado para todos los servidores es 1. Cuanto menor es el número, mayor es el nivel de prioridad.

El presupuesto de alimentación se limita al valor del grupo de las tres unidades de suministro de energía más débiles. Si intenta establecer un valor de presupuesto de alimentación de CA que exceda el *límite de alimentación de entrada del sistema*, la CMC mostrará un mensaje de falla. El límite para el presupuesto de alimentación es 16685 vatios.

Modo de conservación máxima de energía

El CMC realiza una conservación máxima de energía en los siguientes casos:

- El modo de conservación máxima está activado

- Una secuencia de línea de comandos automatizada emitida por una fuente de alimentación ininterrumpible activa el modo de conservación máxima.

En el modo de conservación máxima, todos los servidores comienzan a funcionar a su nivel mínimo de energía y todas las solicitudes posteriores de asignación de energía de servidores se rechazan. En este modo, el rendimiento de los servidores encendidos puede verse reducido. No pueden encenderse servidores adicionales, independientemente de su prioridad.

El sistema se restablece al rendimiento óptimo cuando se desactiva el modo de conservación máxima.

NOTA: Si en el chasis está activado el modo de conservación máxima de energía (MPCM), todas las solicitudes de alimentación de servidores blade se rechazan. Los servidores blade no se encienden si hay alguna acción en la iDRAC o el servidor blade que exija al host iniciar el ciclo de encendido.

Reducción de la alimentación del servidor para mantener el presupuesto de alimentación

La CMC reduce la asignación de alimentación de los servidores de menor prioridad cuando se necesita energía adicional para mantener el consumo de alimentación del sistema dentro del *límite de alimentación de entrada del sistema* configurado por el usuario. Por ejemplo, cuando se conecta un nuevo servidor, la CMC puede reducir la alimentación de los servidores de menor prioridad para obtener más alimentación para el servidor nuevo. Si después de reducir la asignación de alimentación de los servidores de menor prioridad la cantidad de energía aún no es suficiente, la CMC disminuirá el rendimiento de los servidores hasta liberar suficiente energía para alimentar el servidor nuevo.

El CMC reduce la asignación de alimentación a los servidores en dos casos:

- El consumo general de alimentación excede el valor de *Límite de alimentación de entrada del sistema*.
- Se produce una falla de alimentación en una configuración sin redundancia.

Operación de unidades de suministro de energía de 110 V

Algunas unidades de suministro de energía (PSU) admiten la operación con una entrada de 110 V de CA. Esta entrada puede superar el límite permitido para el circuito derivado. Si alguna de las PSU está conectada a 110 V de CA, el usuario deberá configurar la CMC para que el gabinete funcione normalmente. Si no se configura y se detectan PSU de 110 V, todas las solicitudes posteriores de asignación de alimentación de servidores se rechazarán. En ese caso, no podrán encenderse servidores adicionales, independientemente de su prioridad. Puede configurar la CMC para que utilice PSU de 110 V mediante la interfaz web o RACADM.

Las anotaciones del suministro de energía se ingresan en el registro SEL (System Event Log):

- Cuando se detectan o quitan suministros de energía de 110 V.
- Cuando se activa o se desactiva la operación de entrada de 110 V de CA.

Cuando el chasis funciona en modo de 110 V y el usuario no activó dicha operación, la condición general de la alimentación se encuentra como mínimo en estado no crítico. Durante este estado, se muestra el icono de advertencia en la página principal de la interfaz web.

No se admite operación combinada de 110 V y 220 V. Si la CMC detecta ambos voltajes, se selecciona uno de los dos, y los suministros de energía conectados al otro se apagan y se marcan como fallidos.

Rendimiento del servidor sobre redundancia de alimentación

Cuando está activada, esta opción favorece el rendimiento y el encendido de los servidores, por encima del mantenimiento de la redundancia de alimentación. Cuando está desactivada, el sistema favorece la redundancia de alimentación, por encima del rendimiento de los servidores. Cuando está desactivada, si los suministros de energía del chasis no proporcionan suficiente alimentación tanto para redundancia como para rendimiento óptimo, a fin de preservar la redundancia es posible que suceda lo siguiente con algunos servidores:

- No se les otorgue suficiente alimentación para un rendimiento completo
- No se enciendan

Registro remoto

El consumo de alimentación se puede reportar a un servidor syslog remoto. Se puede registrar el consumo total del chasis, y el consumo mínimo, máximo y promedio en un período de recopilación. Para obtener más información sobre cómo activar esta función y configurar el intervalo de recopilación y registro, consulte la sección Ejecución de las operaciones de control de alimentación.

Admin de la alimentación externa

Dell OpenManage Power Center puede controlar la administración de energía del CMC de forma opcional. Para obtener más información, consulte la *Guía del usuario de Dell OpenManage Power Center*.

Cuando se activa la administración de la alimentación externa, el componente **Centro de alimentación de Dell OpenManage** administra:

- Alimentación de servidores de servidores M1000e admitidos
- Prioridad de servidores de servidores M1000e admitidos
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

El CMC sigue manteniendo o administrando lo siguiente:

- Política de redundancia
- Registro remoto de la alimentación
- Rendimiento del sistema sobre redundancia de alimentación
- Conexión dinámica de suministros de energía
- Alimentación del servidor en servidores de 11ª generación y anteriores

Dell OpenManage Power Center administra las prioridades y la alimentación de los servidores M1000e compatibles y los servidores blade posteriores en el chasis con el presupuesto disponible después de la asignación de alimentación a la infraestructura de chasis y los servidores blade de generaciones anteriores. El registro remoto de la alimentación no se ve afectado por la administración de energía externa.

Una vez que el modo de administración de energía basado en servidor esté activado, el chasis estará preparado para la ejecución de la administración de **Dell OpenManage Power Center**. Todas las prioridades de los servidores anteriores y los servidores M1000e compatibles están establecidas en 1 (alta). **Dell OpenManage Power Center** administra directamente las prioridades y la alimentación de los servidores. Dado que **Dell OpenManage Power Center** controla las asignaciones de alimentación de los servidores compatibles, el CMC ya no controla el modo de conservación máxima de alimentación. Por lo tanto, esta opción está desactivada.

Cuando el modo de conservación máxima de alimentación está activado, el CMC establece la capacidad de alimentación de entrada del sistema en el límite máximo que el chasis pueda administrar. El CMC no permite que la alimentación supere la capacidad máxima. Sin embargo, **Dell OpenManage Power Center** maneja todas las demás limitaciones de capacidad de alimentación.

Cuando se desactiva la administración de la alimentación de **Centro de alimentación de Dell OpenManage**, el CMC vuelve a los valores de prioridad de los servidores configurados antes de que se activase la administración externa.

NOTA: Cuando la administración de **Dell OpenManage Power Center** está desactivada, el CMC no realiza la reversión a la configuración anterior de la alimentación máxima del chasis. Consulte el **registro del CMC** para obtener la configuración anterior y restaurar el valor de forma manual.

Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web del CMC

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Para configurar el presupuesto de alimentación mediante la interfaz web:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Alimentación** > **Configuración**. Aparecerá la página **Configuración de redundancia/presupuesto**.
2. Seleccione todas las propiedades que desee de las siguientes. Para obtener información sobre cada uno de los campos, consulte *CMC Online Help (Ayuda en línea de la CMC)*.
   - Activar Administración de alimentación basada en servidor
   - Límite de alimentación de entrada del sistema
   - Política de redundancia
   - Activar Rendimiento de alimentación extendida
   - Activar Rendimiento del servidor sobre redundancia de alimentación
   - Activar conexión dinámica del suministro de energía
   - Desactivar botón de encendido del chasis
   - Permitir operación a 110 VCA
   - Activar Modo de conservación máx. de alimentación
   - Activar registro de alimentación remoto

- Intervalo del registro remoto de la alimentación

3. Haga clic en **Aplicar** para guardar los cambios.

Configuración de la redundancia y el presupuesto de alimentación mediante RACADM

NOTA: Para realizar acciones de administración de la 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), 2 (Redundancia de suministro de energía). El valor predeterminado es 0.

     Por ejemplo, el siguiente comando activa el modo Redundancia de la red eléctrica:

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

   - Para activar o desactivar el modo Rendimiento de alimentación extendida, escriba:

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

     donde <value> es 0 (desactivar), 1 (activar). El valor predeterminado es 1 para las unidades de suministro de energía de 3000 W.

   - Para establecer el valor de Límite de alimentación de entrada del sistema, escriba:

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

     donde <*value*> es un número entre 2715 y 16685 que representa el límite máximo de la alimentación en vatios. El valor predeterminado es 16685.

     Por ejemplo, el siguiente comando establece el valor de Límite de alimentación de entrada del sistema en 5400 vatios:

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
     ```

     .

   - Para activar o desactivar la conexión dinámica de las unidades de suministro de energía, escriba:

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

     donde <*value*> es 0 (desactivar), 1 (activar). El valor predeterminado es 0.

     Por ejemplo, el siguiente comando desactiva el acoplamiento dinámico de unidades de suministro de energía:

     ```
     racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
     ```

     .

   - Para activar la opción Modo de conservación máx. de alimentación, escriba:

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

   - Para restaurar el funcionamiento normal, escriba:

     ```
     racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
     ```

- Active las unidades de suministro de energía de 110 VCA:

  ```
  racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
  ```

- Active Rendimiento del servidor sobre redundancia de alimentación:

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

- Desactive Rendimiento del servidor sobre redundancia de alimentación:

  ```
  racadm config -g cfgChassisPower -o cfgChassisPerformanceOverRedundancy 0
  ```

- Para activar la función de registro remoto de alimentación, escriba el comando siguiente:

  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
  ```

- Para especificar el intervalo de registro deseado, escriba 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, escriba 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 del syslog remoto se hayan configurado previamente. El registro en uno o más hosts del syslog remoto debe estar activado; en caso contrario, se registrará el consumo de energía. Esto puede realizarse a través de la interfaz web o de la CLI de RACADM. Para obtener más información, consulte las instrucciones para la **configuración del syslog remoto** en *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*, disponible en **dell.com/support/manuals**.

- Para activar la opción Administración remota de la alimentación mediante **Centro de alimentación de Dell OpenManage**, escriba:

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

- Para restaurar la administración de la alimentación del CMC, escriba lo siguiente:

  ```
  racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 0
  ```

Para obtener más información acerca de los comandos de RACADM para la alimentación del chasis, consulte las secciones **config**, **getconfig**, **getpbinfo** y **cfgChassisPower** de *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

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.

Conceptos relacionados

Ejecución de operaciones de control de alimentación en el chasis en la página 228
Ejecución de operaciones de control de alimentación en un servidor en la página 228
Ejecución de operaciones de control de alimentación en un módulo de E/S en la página 229

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, el iKVM y las unidades de suministro de energía).

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Ejecución de operaciones de control de alimentación en el chasis mediante la interfaz web

Para ejecutar operaciones de control de alimentación en el chasis mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Alimentación** > **Control**.
   Aparecerá la página **Control de alimentación del chasis**.
2. Seleccione una de las siguientes operaciones de control de alimentación:
   - 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

   Para obtener información sobre cada opción, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
3. Haga clic en **Aplicar**.
   Aparece un cuadro de diálogo que solicita confirmación.
4. Haga clic en **Aceptar** para realizar la acción de administración de la alimentación (por ejemplo, restablecer un 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`.

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.

Ejecución de operaciones de control de alimentación en un servidor

Es posible realizar acciones de administración de alimentación de forma remota para varios servidores a la vez o un servidor individual en el chasis.

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Ejecución de operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC

Para ejecutar operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Alimentación** > **Control**.
   Aparecerá la página **Control de alimentación**.
2. En la columna **Operaciones**, en el menú desplegable, seleccione una de las siguientes operaciones de control de alimentación para los servidores requeridos:
   - Sin operación
   - Encender el servidor
   - Apagar el servidor
   - Apagado ordenado
   - Restablecer el servidor (reinicio mediante sistema operativo)
   - Ciclo de encendido del servidor (reinicio mediante suministro de energía)

   Para obtener más información acerca de estas opciones, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
3. Haga clic en **Aplicar**.
   Aparece un cuadro de diálogo que solicita confirmación.
4. Haga clic en **Aceptar** para realizar la acción de administración de alimentación (por ejemplo, restablecer el servidor).

Ejecución de operaciones de control de alimentación en un servidor mediante la interfaz web del CMC

Para ejecutar operaciones de control de alimentación para un servidor individual mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Descripción general del servidor**.
2. Haga clic en el servidor para el cual desea ejecutar la operación de control de alimentación y, a continuación, haga clic en la ficha **Alimentación**.
   Aparecerá la página **Administración de la alimentación del servidor**.
3. Seleccione una de las siguientes operaciones de control de alimentación:
   - 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 más información acerca de estas opciones, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
4. Haga clic en **Aplicar**.
   Aparece un cuadro de diálogo que solicita confirmación.
5. Haga clic en **Aceptar** para realizar la acción de administración de alimentación (por ejemplo, hacer que el servidor se restablezca).

Ejecución de operaciones de control de alimentación en un servidor mediante RACADM

Para ejecutar operaciones de control de alimentación en un servidor mediante RACADM, abra una consola de texto en serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm serveraction -m <module> <action>
```

donde *<module>* especifica el servidor por su número de ranura (servidor 1 a 16) en el chasis y *<action>* es la operación que desea ejecutar: `powerup`, `powerdown`, `powercycle`, `graceshutdown` o `hardreset`.

Ejecución de operaciones de control de alimentación en un módulo de E/S

Es posible ejecutar de manera remota un restablecimiento o un ciclo de encendido en un módulo de E/S individual.

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Ejecución de operaciones de control de alimentación en módulos de E/S mediante la interfaz web

Para ejecutar operaciones de control de alimentación en un módulo de E/S mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** > **Descripción general del módulo de E/S** y haga clic en **Alimentación**.
   Aparecerá la página **Control de alimentación**.
2. Para el módulo de E/S de la lista, desde el menú desplegable seleccione la operación que desea ejecutar (restablecimiento o ciclo de encendido).
3. Haga clic en **Aplicar**.
   Aparece 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 el módulo de E/S realice un ciclo de encendido).

Ejecución de operaciones de control de alimentación en módulos de E/S mediante RACADM

Para ejecutar operaciones de control de alimentación en un 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-<n><action>
```

donde <*n*> es un número del 1 al 6 y especifica el módulo de E/S (A1, A2, B1, B2, C1, C2), y <acción> indica la operación que desea ejecutar: ciclo de encendido o reinicio.

16

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, el estado de la configuración y los registros históricos de sucesos.

El subcomando `racdump` muestra la siguiente información:

- Información general del sistema/RAC
- Información de la CMC
- Información del chasis
- Información de la sesión
- Información del sensor
- Información de la compilación de firmware

Interfaces admitidas

- RACADM mediante CLI

- RACADM remoto
- RACADM mediante Telnet

Racdump incluye los siguientes subsistemas e incorpora los siguientes comandos RACADM. Para obtener más información sobre racdump, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

Tabla 49. Comandos de racadm para subsistemas

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

Descarga del archivo de base de información de administración de SNMP

El archivo de base de información de administración (MIB) de SNMP de la CMC define los indicadores, sucesos y tipos de chasis. La CMC le permite descargar el archivo de MIB mediante la interfaz web.

Para descargar el archivo MIB SNMP del CMC a través de la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Red** > **Servicios** > **SNMP**.
   Se mostrará la sección **Configuración de SNMP**.
2. Haga clic en **Guardar** para descargar el archivo `MIB` del CMC en su sistema local.

   Para obtener más información sobre el archivo `MIB` SNMP, consulte *Dell OpenManage Server Administrator SNMP Reference Guide (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 está encendido o apagado?
- Si está encendido, ¿el sistema operativo se encuentra en funcionamiento, bloqueado o inmovilizado?
- 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 al menos un suministro de energía del lado 1 (las tres ranuras de la izquierda) y un suministro de energía del lado 2 (las tres ranuras de la derecha) presentes y en estado funcional en el gabinete modular. Además, la capacidad de cada lado debe ser suficiente para admitir el total de asignaciones de energía necesarias para que el chasis mantenga la función **Grid Redundancy (Redundancia de la red eléctrica)**. Para tener funcionamiento completo con redundancia de la red eléctrica, asegúrese de tener disponible una configuración completa de seis unidades de suministro de energía (PSU).
  - **Solución B:** Asegúrese de que todos los suministros de energía estén correctamente conectados a las dos redes de CA. Los suministros del lado 1 deben estar conectados a una red de CA y los del lado 2 deben estar conectados a la otra red, y ambas redes de CA deben estar en funcionamiento. La función **Grid Redundancy (Redundancia de la red eléctrica)** se pierde cuando una de las redes de CA no funciona.
- **Problema:** el estado de la unidad de suministro de energía se muestra como **Error (sin CA),** aun cuando hay conectado un cable de CA y la unidad de distribución de alimentación produce buena salida de CA.
  - **Solución A:** Revise y reemplace el cable de CA. Revise y confirme que la unidad de distribución de energía que proporciona la alimentación al suministro de energía funcione como se espera. Si no se soluciona la falla, comuníquese con el servicio al cliente de Dell para reemplazar el suministro de energía.
  - **Solución B:** revise que la unidad de suministro de energía esté conectada al mismo voltaje que las otras unidades. Si el CMC detecta que una unidad de suministro de energía está funcionando con un voltaje distinto, la unidad se apaga y se marca como fallida.
- **Problema:** la conexión dinámica del suministro de energía está activada, pero ninguno de los suministros de energía se muestra en el modo **En espera**.
  - **Resolución A:** no hay suficiente alimentación excedente. Uno o más suministros de energía pasarán al estado En espera solo cuando el excedente de alimentación disponible en el gabinete supere la capacidad de al menos un suministro de energía.
  - **Solución B:** La conexión dinámica de suministros de energía no es totalmente compatible con las unidades de suministro de energía presentes en el gabinete. Para verificar si es así, utilice la interfaz web para desactivar la función **Dynamic Power Supply Engagement (Conexión dinámica de suministros de energía)** y luego volver a activarla. Si la función no es totalmente compatible, aparecerá un mensaje.
- **Problema:** se instaló un nuevo servidor en el gabinete con suficientes suministros de energía, pero el servidor no se enciende.
  - **Solución A:** asegúrese de que la configuración del límite de alimentación de entrada del sistema no esté demasiado baja para permitir que se enciendan los servidores adicionales.
  - **Solución B:** Verifique el funcionamiento a 110 V. Si hay suministros de energía conectados a circuitos derivados de 110 V, deberá confirmar que se trata de una configuración válida para que los servidores estén autorizados a encenderse. Para obtener más información, consulte los valores de configuración de la alimentación.
  - **Solución C:** Verifique la configuración de la conservación máxima de energía. Si esta opción está activada, los servidores tendrán autorizado encenderse. Para obtener más información, consulte los valores de configuración de la alimentación.
  - **Solución D:** asegúrese de que la prioridad de alimentación de la ranura asociada con el servidor recién instalado no esté por debajo de cualquier otra prioridad de alimentación de ranura del servidor.
- **Problema:** la alimentación disponible cambia continuamente, aun cuando no haya cambiado la configuración de gabinete modular.
  - **Solución:** Las versiones de CMC 1.2 y posteriores tienen administración dinámica de alimentación de ventiladores, la cual reduce brevemente la asignación de alimentación a los servidores si el gabinete opera cerca del límite máximo de alimentación configurado por el usuario. Esto hace que se asigne alimentación a los ventiladores mediante la reducción del rendimiento de los servidores, para mantener el consumo de alimentación de entrada por debajo del valor de **System Input Power Cap (Límite de alimentación de entrada del sistema)**. Este comportamiento es normal.
- **Problema:** 2000 W se consideran como **Excedente para rendimiento pico**.
  - **Solución:** el gabinete tiene 2000 W de alimentación excedente disponible en la configuración actual y el **Límite de alimentación de entrada del sistema** puede ser reducido de forma segura a esta cantidad sin afectar el rendimiento del servidor.
- **Problema:** un subconjunto de servidores perdió alimentación después de una falla de la red de CA, a pesar de que el chasis estaba operando en la configuración **Redundancia de la red eléctrica** con seis suministros de energía.
  - **Solución:** Esto puede ocurrir si los suministros de energía se conectan incorrectamente a las redes de CA redundantes en el momento de la falla en la red de CA. La política de **Grid Redundancy (Redundancia de la red eléctrica)** requiere que los tres suministros de energía de la izquierda estén conectados a una red de CA y los tres de la derecha estén conectados a otra red de CA. Si dos PSU, por ejemplo PSU3 y PSU4, están conectadas a las redes de CA equivocadas, una falla en la red de CA provoca la pérdida de alimentación en los servidores de menor prioridad.
- **Problema:** los servidores de menor prioridad perdieron alimentación después de una falla en una unidad de suministro de energía.
  - **Solución:** Este comportamiento es normal si la política de alimentación del gabinete se configuró en **No Redundancy (Sin redundancia)**. Para evitar que una falla futura en el suministro de energía ocasione que se apaguen los servidores, asegúrese de que el chasis tenga como mínimo cuatro suministros de energía y se configure con la política **Power Supply Redundancy (Redundancia de suministro de energía)**.
- **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 fracaso de cada intento de entrega de capturas de SNMP o de correo electrónico figura en el registro de la CMC. En el registro de rastreo se incluye información adicional para describir cada error. 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.

Conceptos relacionados

Configuración del CMC para enviar alertas en la página 126

Visualización de los registros de sucesos

Es posible ver los registros de hardware y del CMC para obtener información sobre los sucesos críticos del sistema que se producen en el sistema administrado.

Conceptos relacionados

Visualización del registro de hardware en la página 234
Visualización del registro del CMC y del registro mejorado del chasis en la página 235

Visualización del registro de hardware

La CMC genera un registro de los sucesos de hardware que ocurren en el chasis. Para ver el registro de hardware, utilice la interfaz web y RACADM remoto.

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

NOTA: Puede configurar la CMC para enviar capturas SNMP o correos electrónicos cuando ocurran sucesos específicos. Para obtener información sobre la configuración de la CMC para que envíe alertas, consulte Configuración de la CMC para enviar alertas.

Ejemplos de anotaciones en el registro de hardware

```
critical System Software event: redundancy lost
Wed May 09 15:26:28 2007 normal System Software
event: log cleared was asserted
Wed May 09 16:06:00 2007 warning System Software
event: predictive failure was asserted
Wed May 09 15:26:31 2007 critical System Software
event: log full was asserted
Wed May 09 15:47:23 2007 unknown System Software
event: unknown event
```

Conceptos relacionados

Visualización de los registros de sucesos en la página 234

Visualización de los registros de hardware mediante la interfaz web del CMC

Puede ver, guardar y borrar el registro de hardware. También puede ordenar las entradas del registro por gravedad, fecha/hora o descripción si hace clic en el encabezado de la columna. Si se vuelve a hacer clic en el encabezado de la columna se invertirá el orden.

Para ver el registro de hardware mediante la interfaz web de la CMC, en el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **Logs (Registros)** > **Hardware Log (Registro de hardware)**. Aparecerá la página **Hardware Log (Registro de hardware)**. Para guardar una copia del registro de hardware en su red o estación administrada, haga clic en **Save Log (Guardar registro)** y luego especifique una ubicación para el archivo de texto.

NOTA: Debido a que el registro se guarda como archivo de texto, no aparecerán allí las imágenes que se usan para indicar la gravedad en la interfaz de usuario. En el archivo de texto, la gravedad se indica con las palabras OK (Correcto), Informational (Informativo), Unknown (Desconocido), Warning (Advertencia) y Severe (Grave). Las entradas de fecha y hora aparecen en orden ascendente. Si aparece <SYSTEM BOOT> en la columna **Date/Time (Fecha/Hora)**, el suceso ocurrió durante el apagado o el encendido de alguno de los módulos, cuando no había fecha ni hora disponible.

Para borrar el registro de hardware, haga clic en **Borrar registro**.

NOTA: El CMC crea una nueva anotación de registro para indicar que el registro se borró.

Visualización de los registros de hardware mediante RACADM

Para ver el registro de hardware mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getsel
```

Para borrar el registro de hardware, escriba:

```
racadm clrsel
```

Visualización del registro del CMC y del registro mejorado del chasis

La CMC genera un registro de los sucesos relacionados con el chasis y registro mejorado del chasis cuando la opción **Enable Enhanced Logging and Events (Activar registro mejorado y sucesos)** está activada. Para ver el registro mejorado del chasis en la página **Chassis Log (Registro del chasis)**, seleccione la opción **Enable Enhanced Logging and Events (Activar registro mejorado y sucesos)** en la página **General Settings (Configuración general)**. Para activar o desactivar la función mediante RACADM, utilice el objeto `cfgRacTuneEnhancedLog`. Para obtener más información, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)* en **dell.com/support/manuals**.

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

Conceptos relacionados

Visualización de los registros de sucesos en la página 234

Visualización de los registros del CMC mediante la interfaz web

Puede ver, guardar y borrar el registro de la CMC. También puede ordenar las entradas del registro por origen, fecha/hora o descripción si hace clic en el encabezado de la columna. Si se vuelve a hacer clic en el encabezado de la columna se invertirá el orden.

Para ver el registro de la CMC mediante la interfaz web de la CMC, en el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **Logs (Registros)** > **CMC Log (Registro de la CMC)**. Aparecerá la página **CMC Log (Registro de la CMC)**.

Para guardar una copia del registro del CMC en su red o Managed Station, haga clic en **Guardar registro** y luego especifique una ubicación donde guardarlo.

Visualización de los registros del CMC mediante RACADM

Para ver la información del registro del CMC mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getraclog
```

Puede ver el registro mejorado del chasis mediante el comando `racadm chassislog view`

Para borrar el registro del CMC, escriba:

```
racadm clrraclog
```

Visualización de los registros mejorados del chasis mediante la interfaz web

Para ver el registro mejorado del chasis se debe activar la opción **Activar registro mejorado y sucesos** en la página **Configuración general**.

Puede ver todas las actividades del chasis y filtrar, borrar o guardar los registros mediante la página **Registro del chasis** .

Para guardar una copia del registro del CMC en su red o estación de administración, haga clic en **Guardar registro** y luego especifique una ubicación donde guardarlo.

1. Para ver el registro mejorado del chasis mediante la interfaz web de la CMC, en el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)** y haga clic en **Logs (Registros)** > **CMC Log (Registro de la CMC)**. Aparecerá la página **Chassis Log (Registro del chasis)**.
2. En la sección Filtro del registro, seleccione **Tipo de registro** o **Nivel de estado** en el menú desplegable correspondiente o escriba la palabra clave o la fecha en los campos **Búsqueda por palabra clave** y **Rango de Fecha** y luego haga clic en **Aplicar**.
   La tabla Registro del chasis muestra los registros que se clasifican según los filtros seleccionados.
3. Para guardar una copia del registro del chasis en la red o estación de administración, haga clic en **Guardar registro** y luego especifique una ubicación donde guardarlo.

   De manera alternativa, para borrar las anotaciones actuales del registro de hardware, haga clic en **Borrar registro**.

Para obtener más información sobre los demás campos y el uso de la interfaz web, consulte la Ayuda en línea del CMC.

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 del CMC o un usuario bajo la dirección de asistencia técnica.

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

Para obtener acceso a la consola de diagnósticos mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Solución de problemas** > **Diagnóstico**.
   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 *CMC Online Help (Ayuda en línea para el CMC)*.

   Aparecerá una página de resultados de diagnósticos.

Restablecimiento de componentes

Puede restablecer la CMC activa, restablecer la iDRAC sin reiniciar el sistema operativo, o volver a colocar virtualmente los servidores de modo tal que se comporten como si los hubiese quitado y vuelto a insertar. Si el chasis tiene un CMC en espera, el restablecimiento del CMC activo ocasiona una protección contra fallas y el CMC en espera se torna activo.

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

Para restablecer los componentes mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Solución de problemas** > **Restablecer componentes**.
   Aparecerá la página **Restablecer componentes**.
2. Para restablecer la CMC activa, en la sección **CMC Status (Estado de la CMC)**, haga clic en **Reset/Failover CMC (Restablecer/Protección contra fallas de la CMC)**. Si hay una CMC en espera y un chasis totalmente redundante, se produce una protección contra fallas y la CMC en espera se convierte en la activa.
3. Para restablecer la iDRAC solamente, sin reiniciar el sistema operativo, en la sección **Reset Server (Restablecer servidor)**, haga clic en **iDRAC Reset (Restablecimiento de la iDRAC)** en el menú desplegable **Reset (Restablecer)** para los servidores cuya iDRAC

desee restablecer, y luego haga clic en **Apply Selections (Aplicar selecciones)**. De esta manera, se restablecen las iDRAC de los servidores sin reiniciar el sistema operativo.

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

Para restablecer solamente el iDRAC sin reiniciar el sistema operativo mediante RACADM, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e).

NOTA: Cuando se restablece el iDRAC, los ventiladores se establecen al 100% para el servidor.

NOTA: Se recomienda que intente restablecer el iDRAC antes de intentar restablecer virtualmente los servidores.

4. Para restablecer virtualmente el servidor, en la sección **Restablecer servidor**, haga clic en **Recolocación virtual** en el cuadro desplegable **Restablecer** correspondiente a los servidores que desea volver a colocar y luego haga clic en **Aplicar selecciones**.

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

   Esta operación hace que los servidores se comporten como si se hubiesen quitado e insertado nuevamente.

Guardar o restaurar la configuración del chasis

Para guardar o restaurar una copia de seguridad de la configuración del chasis con la interfaz web del CMC, en el árbol del sistema, diríjase a **Descripción general del chasis** y haga clic en **Configuración** > **Copia de seguridad del chasis**

Aparecerá la página **Copia de seguridad del chasis**.

Para guardar la configuración del chasis, haga clic en **Save (Guardar)**. Modifique la ruta predeterminada de acceso al archivo (opcional) y haga clic en **OK (Aceptar)** para guardar el archivo.

NOTA: El nombre predeterminado del archivo de la copia de seguridad contiene la etiqueta de servicio del chasis. Este archivo de copia de seguridad puede utilizarse más adelante para restaurar la configuración y los certificados únicamente en este chasis.

Para restaurar la configuración del chasis, haga clic en **Elegir archivo**, especifique el archivo de copia de seguridad y haga clic en **Restaurar**.

NOTA:

- La CMC no se restablece al restaurar la configuración; sin embargo, los servicios de la CMC pueden tardar un poco en aplicar la nueva configuración. Una vez que el proceso se complete correctamente, se cerrarán todas las sesiones actuales.
- La información de Flexaddress, perfiles de servidor y almacenamiento extendido no se guardan ni se restauran con la configuración del chasis.

Solución para errores de protocolo de hora de red

Después de configurar la CMC de modo que el reloj se sincronice con un servidor de hora remoto por la red, pueden transcurrir de 2 a 3 minutos hasta que se refleje el cambio en la fecha y hora. Si transcurrido este tiempo no se produce ningún cambio, es posible que sea necesario solucionar algún problema. La CMC quizás no puede sincronizar el reloj por las siguientes razones:

- Es posible que haya un problema con los valores de Servidor NTP 1, Servidor NTP 2 y Servidor NTP 3.
- Es posible que se haya introducido accidentalmente un nombre de host o una dirección IP no válidos.
- Es posible que haya un problema de conectividad de red que impida que el CMC se comunique con alguno de los servidores NTP configurados.
- Podría existir un problema de DNS que impida que se resuelvan algunos nombres de host del servidor NTP.

Para solucionar los problemas relacionados con NTP, revise el registro de rastreo de la CMC. Este registro contiene mensajes 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` de `ntpd`. Antes de cambiar este parámetro, entienda todas las consecuencias, ya que el valor predeterminado debe ser lo suficientemente alto para funcionar 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 introducir el comando `gettracelog` para revisar el registro de rastreo mediante la interfaz web de la CMC, consulte Uso de la consola de diagnósticos.

Interpretación de los colores y los patrones de parpadeo de los LED

Los LED en el chasis proporcionan la siguiente información de estado sobre los componentes:

- Los LED que se mantienen encendidos en color verde indican que el componente está encendido. Si el LED verde parpadea, indica un suceso crítico pero de rutina, como una carga de firmware, durante la cual la unidad no se encuentra en funcionamiento. No indica una falla.
- Los LED que parpadean en color ámbar en un módulo indican una falla en ese módulo.
- Los LED que parpadean en color azul pueden ser configurados por el usuario y utilizados para la identificación. Para obtener más información acerca de la configuración, consulte Descarga del archivo de base de información de administración (MIB) de SNMP.

Tabla 50. Colores y patrones de parpadeo de los LED

Componente	Color de LED, patrón de parpadeo	Estado
CMC	Verde, encendido permanentemente	No se enciendan
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Activo
	Azul, parpadeante	Identificador de módulo activado por el usuario

Tabla 50. Colores y patrones de parpadeo de los LED (continuación)

Componente	Color de LED, patrón de parpadeo	Estado
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Modo de espera
iKVM	Verde, encendido permanentemente	No se enciendan
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Ámbar, apagado	Sin fallas
Servidor	Verde, encendido permanentemente	No se enciendan
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas
Módulo de E/S (común)	Verde, encendido permanentemente	No se enciendan
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal/maestro de apilamiento
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas/esclavo de apilamiento
Módulo de E/S (de paso)	Verde, encendido permanentemente	No se enciendan
	Verde, parpadeante	No se utiliza
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas
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

Tabla 50. Colores y patrones de parpadeo de los LED (continuación)

Componente	Color de LED, patrón de parpadeo	Estado
	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

Solución de problemas de un CMC que no responde

Si no puede iniciar sesión en el CMC por medio de ninguna de las interfaces (interfaz web, Telnet, SSH, RACADM remoto o serie), puede verificar la funcionalidad del CMC mediante la observación de sus indicadores LED en CMC, la obtención de información de recuperación con el puerto serie DB-9 o la recuperación de la imagen del firmware del CMC.

NOTA: No es posible iniciar sesión en el CMC en espera por medio de una consola serie.

Observación de los LED para aislar el problema

Poniéndose de frente del CMC, tal y como está instalado en el chasis, verá dos indicadores LED a la izquierda de la tarjeta:

- LED superior: El LED verde superior indica alimentación. Si no está encendido:
  - Verifique que haya corriente alterna presente en al menos un suministro de energía.
  - Verifique que la tarjeta de la CMC esté instalada correctamente. Puede liberar o tirar de la palanca de expulsión, extraer la CMC y volver a instalarla asegurándose de que la placa se inserte por completo y el seguro cierre correctamente.
- LED inferior: El LED inferior tiene varios colores. Cuando la CMC está activa y en funcionamiento, y no hay ningún problema, el LED inferior está en azul. Si está de color ámbar, se ha detectado una falla. La falla podría ser a causa de cualquiera de estos tres sucesos:
  - Una falla del núcleo. En este caso, se debe reemplazar la placa de la CMC.
  - Una falla de autoprueba. En este caso, se debe reemplazar la placa de la CMC.
  - Una imagen dañada. En este caso, cargue la imagen del firmware de la CMC para recuperar la CMC.

  NOTA: Un inicio o restablecimiento normal de la CMC demora poco más de un minuto en iniciar el sistema operativo y permitir el inicio de sesión. Se activará el LED azul en la CMC activa. En una configuración redundante de dos CMC, solo se activa el LED verde en la CMC en espera.

Obtención de la información de recuperación desde el puerto serie DB-9

Si el LED inferior es de color ámbar, la información de recuperación está disponible en el puerto serie DB-9, que se ubica en el frente del CMC.

Para obtener la información de recuperación:

1. Instale un cable de módem NULO entre el CMC y la máquina cliente.
2. Abra el emulador de terminal que prefiera (como HyperTerminal o Minicom). Configure los siguientes valores: 8 bits, sin paridad, sin control de flujo, y velocidad en baudios 115200.
   La falla de la memoria del núcleo muestra un mensaje de error cada 5 segundos.
3. Presione <Intro>.

Si aparece una petición de recuperación, hay disponible información adicional. La petición indica el número de ranura de la CMC y el tipo de falla.

Para ver el motivo de la falla y la sintaxis de algunos comandos, escriba `recover` y presione <Intro>.

Peticiones de ejemplo:

```
recover1[self test] CMC 1 self test failure
```

```
recover2[Bad FW images] CMC2 has corrupted images
```

- Si la petición indica una falla de autoprueba, no hay componentes reparables en la CMC. La CMC está dañada y se debe regresar a Dell.
- Si la petición indica **Imágenes de firmware dañadas**, siga los pasos que se indican en Recovering Firmware Image (Recuperación de la imagen del firmware) para resolver el problema.

Recuperación de la imagen del firmware

La CMC pasa al modo de recuperación cuando no es posible el inicio operativo normal de la CMC. En el modo de recuperación, hay disponible un pequeño subconjunto de comandos que permite reprogramar los dispositivos flash mediante la carga del archivo de actualización del firmware, `firmimg.cmc`. Este es el mismo archivo de imagen del firmware que se utiliza para las actualizaciones normales del firmware. El proceso de recuperación muestra su actividad actual y, una vez que se completa, genera un inicio en el SO de la CMC.

Cuando escribe recover y luego presiona <Intro> en la petición de recuperación, aparecen el motivo de la recuperación y los subcomandos disponibles. Un ejemplo de secuencia de recuperación podría ser:

```
recover getniccfg
recover setniccfg 192.168.0.120 255.255.255.0
192.168.0.1
recover ping 192.168.0.100
recover fwupdate -g -a 192.168.0.100
```

NOTA: Conecte el cable de red al conector RJ45 del extremo izquierdo.

NOTA: En el modo de recuperación, no puede enviar comandos ping a la CMC con normalidad porque no hay ningún apilamiento de red activo. El comando `recover ping <TFTP server IP>` le permite enviar comandos ping al servidor TFTP para verificar la conexión de LAN. Es posible que necesite utilizar el comando `recover reset` después de `setniccfg` en algunos sistemas.

Solución de problemas de red

El registro de rastreo interno de la CMC le permite depurar el sistema de red y las alertas 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 *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*.

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.

Restablecimiento de la contraseña de administrador

PRECAUCIÓN: Muchas de las reparaciones deben ser realizadas únicamente por un técnico de servicio autorizado. El usuario debe llevar a cabo únicamente las tareas de solución de problemas y las reparaciones sencillas autorizadas en la documentación del producto o indicadas por el personal de servicio y de asistencia en línea o telefónica. 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, hace falta un usuario con privilegios de **Administrador**. El software de la CMC tiene una función de seguridad para la protección de la contraseña de la cuenta del usuario que puede desactivarse si se olvida la contraseña de la cuenta del administrador. Si se olvida la contraseña de la cuenta del administrador, se puede recuperar mediante el puente PASSWORD_RSET en la placa de la CMC.

El puente de la CMC tiene un conector de restablecimiento de contraseña de dos clavijas, tal como se muestra en la siguiente figura. Si se instala un puente en el conector de restablecimiento, la cuenta y contraseña predeterminadas del administrador se activan con los valores predeterminados `username: root` y `password: calvin`. La cuenta del administrador se restablecerá independientemente de si se eliminó la cuenta o se cambió la contraseña.

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

Para realizar acciones de administración, hace falta un usuario con privilegios de **Administrador**. Si se olvida la contraseña de la cuenta del administrador, se puede restablecer mediante el puente PASSWORD_RST 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 del asa de la CMC y aleje el asa del panel frontal del módulo. Extraiga el módulo CMC del gabinete.

   NOTA: Las descargas electroestáticas (ESD) pueden dañar la CMC. En determinadas condiciones, las ESD pueden acumularse en el cuerpo o en algún objeto y luego descargarse en la CMC. Para evitar daños ocasionados por ESD, tome las precauciones necesarias para descargar toda electricidad estática de su cuerpo antes de manipular o acceder a la CMC fuera del chasis.

2. Quite el tapón del puente del conector de restablecimiento de contraseña e inserte un puente de dos clavijas para activar la cuenta predeterminada del administrador. Consulte la siguiente figura para localizar el puente de contraseña en la placa de la CMC.

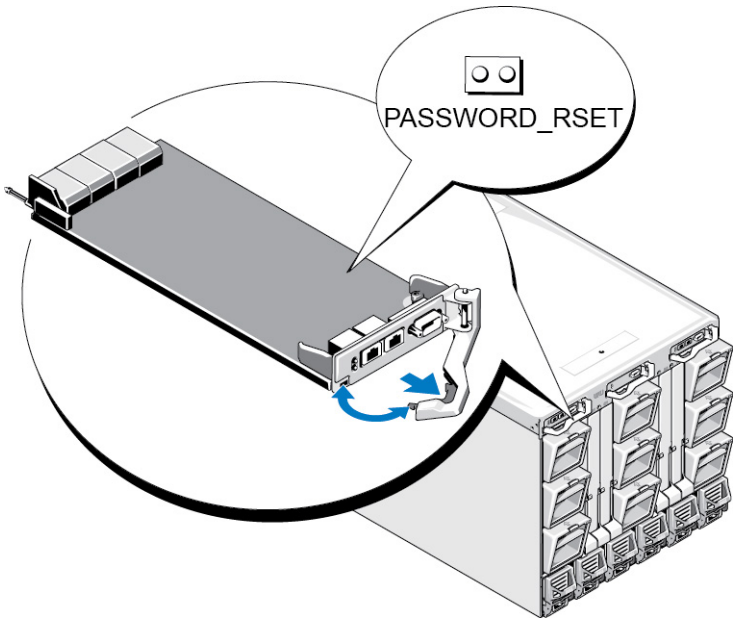


Ilustración 18. Ubicación del puente de restablecimiento de contraseña

Tabla 51. Opciones del puente de contraseña del CMC

PASSWORD_RST		(predeter minada)	La función de restablecimiento de contraseña está desactivada.
			La función de restablecimiento de contraseña está activada.

3. Inserte el módulo de la CMC en el gabinete. Vuelva a conectar los cables que se desconectaron.

   NOTA: Asegúrese de que el módulo CMC se convierta en el CMC activo y que siga en ese estado hasta completar los pasos restantes.

4. Si el módulo de la CMC cuyo puente utilizó es la única CMC, espere a que se complete el reinicio. Si hay una CMC redundante en el chasis, inicie un cambio para que el módulo de la CMC cuyo puente utilizó se convierta en la CMC activa. En la interfaz web, en el árbol del sistema, vaya a **Chassis Overview (Descripción general del chasis)**, haga clic en **Power (Alimentación)** > **Control**, seleccione **Reset CMC (warm boot) (Restablecer CMC, inicio mediante sistema operativo)** y haga clic en **Apply (Aplicar)**. El CMC cederá automáticamente sus funciones al módulo redundante y este último se convertirá en el módulo activo.
5. Inicie sesión en la CMC activa con el nombre de usuario y la contraseña de administrador predeterminados, root y calvin, y restaure los valores de configuración que necesite de la cuenta de usuario. Las cuentas y contraseñas existentes no están desactivadas; permanecen activadas.
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 del asa de la CMC y aleje el asa del panel frontal del módulo. Extraiga el módulo CMC del gabinete.
   b. Quite el puente de dos clavijas y vuelva a colocar el tapón del puente.
   c. Inserte el módulo de la CMC en el gabinete. Vuelva a conectar los cables que se desconectaron. Repita el paso 4 para que el módulo de la CMC cuyo puente no utilizó sea la CMC activa.

17

Uso de la interfaz del panel LCD

El panel LCD del chasis puede utilizarse para realizar tareas de configuración y diagnóstico, y para obtener información de estado acerca del chasis y su contenido.

En la siguiente figura se ilustra el panel LCD. La pantalla LCD muestra menús, iconos, imágenes y mensajes.

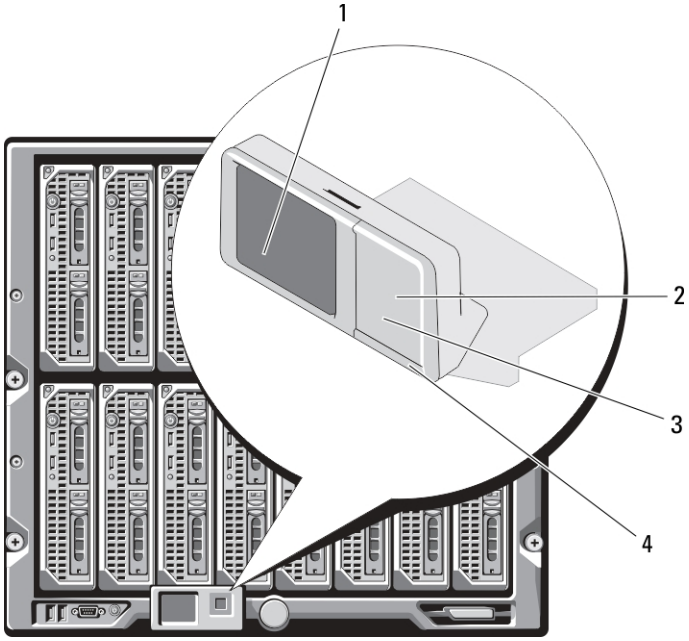


Ilustración 19. Pantalla LCD

Tabla 52. Pantalla LCD: componentes

1	Pantalla LCD	2	Botón de selección ("check")
3	Botones de desplazamiento (4)	4	LED indicador de estado

Conceptos relacionados

Navegación de la pantalla LCD en la página 245
Diagnóstico en la página 248
Solución de problemas del hardware de LCD en la página 248
Mensajes de la pantalla LCD del panel frontal en la página 250
Mensajes de error de la pantalla LCD en la página 250
Información de estado del servidor y del módulo de LCD en la página 254

Temas:

Navegación de la pantalla LCD

El lado derecho del panel LCD tiene cinco botones: cuatro botones de flecha (arriba, abajo, izquierda y derecha) y un botón central.

- *Para desplazarse entre pantallas, use los botones de flecha hacia la derecha (siguiente) e izquierda (anterior). Mientras se usa el panel, siempre es posible regresar a una pantalla anterior.*
- *Para desplazarse a través de las opciones en una pantalla, utilice los botones de flecha hacia abajo y arriba.*
- *Para seleccionar y guardar un elemento en una pantalla y avanzar a la siguiente pantalla, utilice el botón central.*

Los botones de flecha hacia arriba, abajo, izquierda y derecha cambian los iconos o elementos de menú seleccionados en la pantalla. El elemento seleccionado se muestra con un fondo o borde celeste.

Si la longitud de los mensajes que se muestran en la pantalla LCD excede la capacidad de la pantalla, utilice los botones de flecha hacia la izquierda y la derecha para desplazarse por el texto en esas direcciones.

Los iconos que se describen en la tabla siguiente se usan para navegar por las pantallas LCD.

Tabla 53. Iconos de navegación del panel LCD

Icono normal	Icono resaltado	Nombre y descripción del icono
		**Atrás**: seleccione y presione el botón central para regresar a la pantalla anterior.
		**Aceptar/Sí**: seleccione y presione el botón central para aceptar un cambio y regresar a la pantalla anterior.
		**Omitir/Siguiente**: seleccione y presione el botón central para omitir los cambios y avanzar a la siguiente pantalla.
		**No**: seleccione y presione el botón central para responder "No" a una pregunta y avanzar a la siguiente pantalla.
		**Rotar**: seleccione y presione el botón central para alternar entre las vistas gráficas de la parte frontal y posterior del chasis. **NOTA:** El fondo de color ámbar indica que la vista opuesta contiene errores.
		**Identificación del componente**: parpadea el LED azul en un componente. **NOTA:** Se muestra un rectángulo azul parpadeante cerca de este icono cuando se activa la opción Identificación del componente.

El LED indicador de estado en el panel LCD indica la condición general del chasis y de sus componentes.

- Azul continuo indica que está en buenas condiciones.
- Parpadeo en color ámbar indica que al menos un componente tiene una condición de falla.
- Parpadeo en color azul es una señal de identificación que se utiliza para identificar un chasis en un grupo de chasis.

Conceptos relacionados

Menú principal en la página 246
Menú de configuración de LCD en la página 246
Pantalla de configuración de idioma en la página 246
Pantalla predeterminada en la página 246
Pantalla de estado gráfico del servidor en la página 247
Pantalla de estado gráfico del módulo en la página 247
Pantalla del menú Gabinete en la página 247
Pantalla de estado del módulo en la página 247

Pantalla Estado del gabinete en la página 248
Pantalla Resumen de IP en la página 248

Menú principal

Desde **Menú principal**, es posible obtener acceso a una de las siguientes pantallas:

- **Menú de configuración de LCD**: seleccione el idioma que se utilizará y la pantalla LCD que aparecerá cuando no se utilice el LCD.
- **Servidor**: muestra información sobre el estado de los servidores.
- **Gabinete**: muestra información sobre el estado del chasis.

Use los botones de flecha hacia arriba y abajo para resaltar una opción.

Para activar la opción seleccionada, presione el botón central.

Menú de configuración de LCD

El menú **Configuración de LCD** muestra diversas opciones que pueden configurarse:

- **Configuración de idioma**: seleccione el idioma que desea utilizar para el texto de la pantalla LCD y los mensajes.
- **Pantalla predeterminada**: elija la pantalla que aparece cuando el panel LCD está inactivo.

Utilice los botones de flecha hacia arriba y abajo para resaltar una opción del menú, o para resaltar el icono **Back (Atrás)** si desea regresar al menú **Main (Principal)**.

Para activar la opción seleccionada, presione el botón central.

Pantalla de configuración de idioma

La pantalla **Language Setup (Configuración de idioma)** le permite seleccionar el idioma usado para los mensajes del panel LCD. El idioma actualmente activo está resaltado con un fondo celeste.

1. Use los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia la derecha para resaltar el idioma deseado.
2. Presione el botón central.

   Aparecerá el icono **Aceptar** resaltado.
3. Para confirmar el cambio, presione el botón central.

   Aparecerá el menú **Configuración de LCD**.

Pantalla predeterminada

Default Screen (Pantalla predeterminada) le permite cambiar la pantalla que el panel LCD muestra cuando no hay actividad en el panel. La pantalla predeterminada de fábrica es **Main Menu (Menú principal)**. Puede elegir entre las siguientes pantallas:

- **Menú principal**
- **Estado del servidor** (vista frontal del chasis)
- **Estado del módulo** (vista posterior del chasis)
- **Personalizado** (logotipo de Dell con nombre del chasis)

La pantalla actualmente activa aparece resaltada en celeste.

1. Utilice los botones de flecha hacia arriba y abajo para resaltar la pantalla que desea definir como predeterminada.
2. Presione el botón central.

   El icono **Aceptar** quedará resaltado.
3. Presione el botón central nuevamente para confirmar el cambio.

   Aparecerá la **Pantalla predeterminada**.

Pantalla de estado gráfico del servidor

La pantalla **Graphical Server Status (Estado gráfico de servidores)** muestra iconos para cada servidor instalado en el chasis e indica la condición general de cada uno. La condición del servidor se indica mediante el color del icono del servidor:

- Gris: el servidor está apagado y no presenta errores.
- Verde: el servidor está encendido y no presenta errores.
- Amarillo: se han producido uno o varios errores no críticos en el servidor.
- Rojo: se han producido uno o varios errores críticos en el servidor.
- Negro: no se registra la presencia del servidor.

El rectángulo azul que parpadea alrededor del icono de servidor indica el servidor seleccionado.

Para ver la pantalla **Estado gráfico del módulo**, seleccione el icono de rotación y presione el botón central.

Para ver la pantalla de estado de un servidor, use los botones de flecha para seleccionar el servidor que desee y presione el botón central. Aparecerá la pantalla **Server Status (Estado del servidor)**.

Para regresar a Menú principal, use los botones de flecha para seleccionar el icono **Atrás** y presione el botón central.

Pantalla de estado gráfico del módulo

La pantalla **Graphical Module Status (Estado gráfico de los módulos)** muestra todos los módulos instalados en la parte posterior del chasis y ofrece un resumen de la condición de cada uno. La condición de los módulos se indica mediante el color de cada icono de módulo de la siguiente forma:

- Gris: el módulo está apagado o en espera y no presenta errores.
- Verde: el módulo está encendido y no presenta errores.
- Amarillo: se han producido uno o varios errores no críticos en el módulo.
- Rojo: se han producido uno o varios errores críticos en el servidor.
- Negro: no se registra la presencia del módulo.

El rectángulo azul que parpadea alrededor del icono de módulo indica el módulo seleccionado.

Para ver la pantalla **Estado gráfico del servidor**, seleccione el icono de rotación y presione el botón central.

Para ver la pantalla de estado de un módulo, use los botones de flecha hacia arriba, abajo, derecha e izquierda para seleccionar el módulo que desee y presione el botón central. Aparecerá la pantalla **Module Status (Estado del módulo)**.

Para regresar a **Main Menu (Menú principal)**, use los botones de flecha para seleccionar el icono Back (Atrás) y presione el botón central. Aparecerá **Main Menu (Menú principal)**.

Pantalla del menú Gabinete

Esta pantalla permite obtener acceso a las siguientes pantallas:

- **Pantalla Estado del módulo**
- **Pantalla Estado del gabinete**
- **Pantalla Resumen de IP**
- **Menú principal**

Use los botones de navegación para seleccionar el elemento que desee (seleccione el icono **Back [Atrás]** para regresar a **Main Menu [Menú principal]**) y presione el botón central. Se mostrará la pantalla seleccionada.

Pantalla de estado del módulo

La pantalla **Module Status (Estado del módulo)** muestra la información y los mensajes de error de un módulo. Para ver los mensajes que pueden aparecer en esta pantalla, consulte Información de estado del servidor y del módulo de LCD y Mensajes de error de la pantalla LCD.

Use las teclas de flecha hacia arriba y abajo para moverse por los mensajes. Utilice las teclas de flecha hacia la izquierda y la derecha para desplazarse por los mensajes que no caben en la pantalla.

Seleccione el icono **Atrás** y presione el botón central para regresar a la pantalla **Estado gráfico del módulo**.

Pantalla Estado del gabinete

La pantalla **Enclosure Status (Estado del gabinete)** muestra la información y los mensajes de error del gabinete. Para ver los mensajes que pueden aparecer en esta pantalla, consulte Mensajes de error de la pantalla LCD. Use las teclas de flecha hacia arriba y abajo para moverse por los mensajes.

Utilice las teclas de flecha hacia la izquierda y la derecha para desplazarse por los mensajes que no caben en la pantalla.

Seleccione el icono **Atrás** y presione el botón central para regresar a la pantalla **Estado del gabinete**.

Pantalla Resumen de IP

La pantalla **Resumen de IP** muestra información de IP del CMC y el iDRAC de cada servidor instalado.

Use los botones de flecha hacia arriba y abajo para desplazarse por la lista. Use los botones de flecha hacia la izquierda y derecha para desplazarse por los mensajes seleccionados que no caben en la pantalla.

Use los botones de flechas hacia arriba y hacia abajo para seleccionar el icono **Atrás** y presione el botón central para regresar al menú **Gabinete**.

Diagnóstico

El panel LCD lo ayuda a diagnosticar problemas en cualquier servidor o módulo del chasis. Si hay un problema o una falla en el chasis, en cualquier servidor o en otro módulo del chasis, el indicador de estado del panel LCD parpadea en color ámbar. En el menú principal, aparece junto al elemento del menú (servidor o gabinete) un icono con fondo ámbar que conduce al servidor o módulo con problemas.

Siguiendo los iconos color ámbar a través del sistema de menús de la pantalla LCD, es posible visualizar la pantalla de estado y los mensajes de error del elemento que presenta el problema.

Los mensajes de error del panel LCD pueden quitarse eliminando el módulo o el servidor que causa el problema o borrando el registro de hardware del módulo o servidor. En los casos de errores de servidor, use la interfaz de línea de comandos o la interfaz web de la iDRAC para borrar el registro de sucesos del sistema (SEL) del servidor. En los casos de errores de chasis, use la interfaz de línea de comandos o la interfaz web de la CMC para borrar el registro de hardware.

Solución de problemas del hardware de LCD

Si tiene problemas con el LCD que estén relacionados con el uso del CMC, utilice las siguientes opciones de solución de problemas de hardware para determinar si existe un problema con el hardware de LCD o con la conexión.

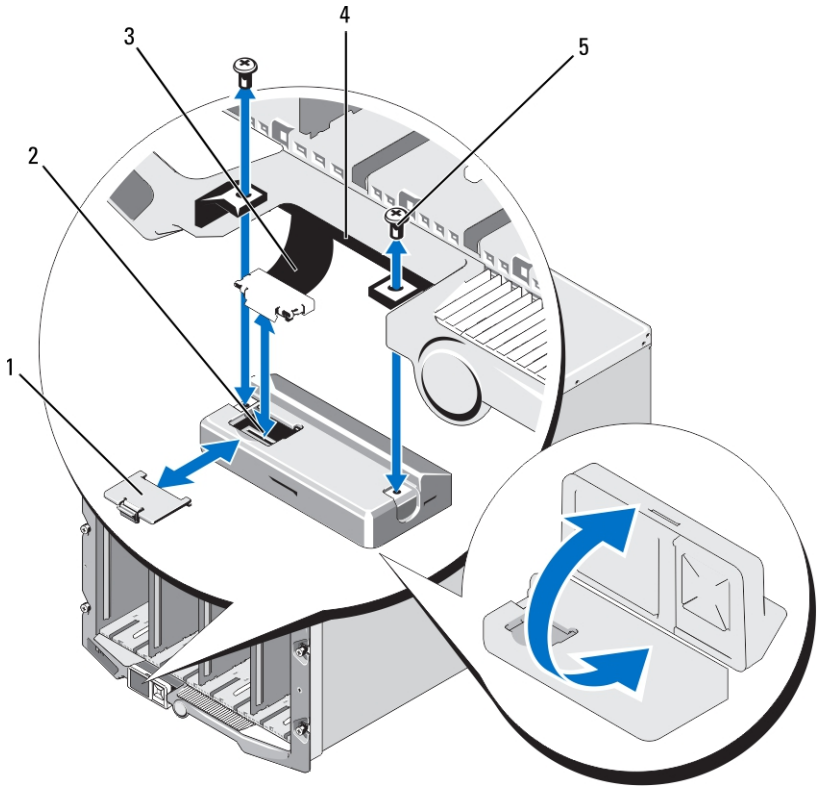


Ilustración 20. Extracción e instalación del módulo LCD

Tabla 54. Módulo LCD: componentes

1	la cubierta de cables	2	módulo LCD
3	Cable plano	4	Bisagras (2)
5	Tornillos (2)		

Tabla 55. Elementos de solución de problemas del hardware de LCD

Síntoma	Problema	Acción de recuperación
Pantalla con mensaje de alerta `CMC Not Responding` y LED parpadeando en color ámbar.	Se produce una pérdida de la comunicación del CMC al panel frontal del LCD.	Verifique que el CMC se esté iniciando; luego, reinicie el CMC a través de la interfaz gráfica de usuario o los comandos de RACADM.
Pantalla con mensaje de alerta `CMC Not Responding` y LED de color ámbar o apagado.	Se ha producido un error en la comunicación del módulo LCD durante un reinicio o una protección contra fallas del CMC.	Revise el registro de hardware mediante la GUI o comandos RACADM. Busque el mensaje `Can not communicate with LCD controller.` Vuelva a colocar el cable plano del módulo LCD.
El texto de la pantalla está codificado.	Pantalla LCD defectuosa.	Sustituya el módulo LCD.
El LED y el LCD están apagados.	El cable LCD no está conectado correctamente o no funciona; o el módulo LCD no funciona.	Revise el registro de hardware mediante la GUI o comandos RACADM. Busque este mensaje: • `The LCD module cable is not connected, or is improperly connected.` • `The control panel cable is not connected, or is improperly connected.` Vuelva a colocar los cables.

Tabla 55. Elementos de solución de problemas del hardware de LCD (continuación)

Pantalla LCD con el mensaje `No CMC Found.`	No hay ningún CMC en el chasis.	Inserte un CMC en el chasis o vuelva a colocar el CMC existente, si hay uno.

Mensajes de la pantalla LCD del panel frontal

Esta sección incluye dos apartados que muestran los mensajes de error y la información de estado que aparecen en la pantalla LCD del panel frontal.

Los *mensajes de error* de la pantalla LCD tienen un formato similar al del registro de sucesos del sistema (SEL) que se visualiza en la interfaz web o en CLI.

Las tablas en la sección de errores muestran los mensajes de error y de advertencia que aparecen en las diferentes pantallas LCD y la causa posible de cada mensaje. El texto entre corchetes angulares (< >) puede variar.

La *información de estado* en la pantalla LCD incluye información descriptiva sobre los módulos del chasis. Las tablas en esta sección describen la información que se muestra para cada componente.

Mensajes de error de la pantalla LCD

Tabla 56. Pantallas de estado del CMC

Gravedad	Mensaje	Causa
Crítico	Falló la batería <número> del CMC.	La batería de CMOS del CMC no está presente o no tiene voltaje.
Crítico	Se perdió el pulso de la LAN <número> del CMC.	Se eliminó la conexión NIC del CMC o no está conectada.
Aviso	A firmware or software incompatibility detected between iDRAC in slot <number> and CMC. (Se ha detectado una incompatibilidad de firmware o de software entre el iDRAC de la ranura <number> y la CMC).	El firmware entre los dos dispositivos no coincide para poder admitir a una o varias funciones.
Aviso	A firmware or software incompatibility detected between system BIOS in slot <number> and CMC. (Se ha detectado una incompatibilidad de firmware o de software entre el BIOS del sistema de la ranura <number> y la CMC).	El firmware entre los dos dispositivos no coincide para poder admitir a una o varias funciones.
Aviso	Se ha detectado una incompatibilidad de firmware o software entre CMC 1 y CMC 2.	El firmware entre los dos dispositivos no coincide para poder admitir a una o varias funciones.

Tabla 57. Pantalla de estado del gabinete/chasis

Gravedad	Mensaje	Causa
Crítico	Se quitó el ventilador <número>.	Este ventilador es necesario para la correcta ventilación del gabinete o del chasis.
Aviso	Se ha degradado la redundancia del suministro de energía.	Una o más unidades de suministro de energía fallaron o fueron eliminadas, y el sistema ya no admite la redundancia de unidad de suministro de energía total.
Crítico	Se ha perdido la redundancia de la fuente de alimentación.	Una o más unidades de suministro de energía fallaron o fueron eliminadas, y el sistema ya no es redundante.
Crítico	Las fuentes de alimentación no son redundantes. Los recursos son insuficientes para mantener las operaciones normales.	Una o más unidades de suministro de energía fallaron o fueron eliminadas, y el sistema carece de suficiente energía para mantener el funcionamiento normal. Esto puede provocar que se apaguen los servidores.
Aviso	La temperatura ambiente del panel de control está por arriba del umbral máximo de advertencia.	La temperatura de entrada del chasis o del gabinete está por arriba del umbral de advertencia.

Tabla 57. Pantalla de estado del gabinete/chasis (continuación)

Gravedad	Mensaje	Causa
Crítico	La temperatura ambiente del panel de control está por arriba del umbral máximo de advertencia.	La temperatura de entrada del chasis o del gabinete está por arriba del umbral de advertencia.
Crítico	Se perdió la redundancia de CMC.	La CMC ya no es redundante. Esto sucede cuando se elimina la CMC en espera.
Crítico	Se ha desactivado el registro de todos los eventos.	El chasis o el gabinete no pueden almacenar sucesos en los registros. En general, esto indica que hay un problema con el panel de control o con el cable del panel de control.
Aviso	Log is full.	El chasis detectó que solo se puede agregar una entrada más al CEL (registro de hardware) para que esté lleno.
Aviso	El registro está casi lleno.	El registro de sucesos del chasis se encuentra al 75% de su capacidad.

Tabla 58. Pantallas de estado del ventilador

Gravedad	Mensaje	Causa
Crítico	El ventilador <número> está funcionando a una velocidad en RPM por debajo del umbral crítico mínimo.	La velocidad del ventilador especificado no es suficiente para proporcionar ventilación adecuada al sistema.
Crítico	El ventilador <número> está funcionando a una velocidad en RPM por arriba del umbral crítico máximo.	La velocidad del ventilador especificado es demasiado alta, lo que normalmente se debe a que una de las aspas del ventilador está rota.

Tabla 59. Pantallas de estado del módulo de E/S

Gravedad	Mensaje	Causa
Aviso	Se produjo una incompatibilidad de la red Fabric en el módulo de E/S <número>.	La red Fabric del módulo de E/S no coincide con la del servidor o la del módulo de E/S redundante.
Aviso	Se detectó una falla de sintonía de vínculos en el módulo de E/S <número>.	El módulo de E/S no se pudo configurar correctamente para utilizar el NIC en uno o varios servidores.
Crítico	Se produjo una falla en el módulo de E/S <número>.	El módulo de E/S presenta una falla. El mismo error puede ocurrir si se produce un disparo térmico en el módulo de E/S.

Tabla 60. Pantalla de estado de iKVM

Gravedad	Mensaje	Causa
Aviso	La consola no está disponible para el KVM local.	Falla menor, por ejemplo, el firmware está dañado.
Crítico	El KVM local no puede detectar ningún host.	Falla en la enumeración de host USB.
Crítico	El protocolo OSCAR, que aparece en la pantalla, no está operativo para el KVM local.	Falla en el protocolo OSCAR.
No es recuperable.	El KVM local no está operativo y está apagado.	Falla en la serie de RIP o en el chip del host USB.

Tabla 61. Pantallas de estado de la unidad de suministro de energía

Gravedad	Mensaje	Causa
Crítico	Power supply <number> failed. (Se ha producido un error en la fuente de alimentación <número>).	Se produjo una falla en la unidad de suministro de energía.
Crítico	The power input for power supply <number> is lost. (Se ha perdido la entrada de corriente de la fuente de alimentación <número>).	Pérdida de energía de CA o cable de CA sin conectar.

Tabla 61. Pantallas de estado de la unidad de suministro de energía (continuación)

Gravedad	Mensaje	Causa
Aviso	Power supply <number> is operating at 110 volts, and could cause a circuit breaker fault. (El suministro de energía <number> está funcionando a 110 voltios y esto podría producir un error en el interruptor de circuito).	El suministro de energía está conectado a una fuente de alimentación de 110 voltios.

Tabla 62. Pantalla de estado del servidor

Gravedad	Mensaje	Causa
Aviso	La temperatura ambiente de la placa del sistema está por debajo del umbral de advertencia mínimo.	La temperatura del servidor está bajando.
Crítico	La temperatura ambiente de la placa del sistema está por debajo del umbral crítico mínimo.	La temperatura del servidor está disminuyendo.
Aviso	La temperatura ambiente de la placa del sistema está por arriba del umbral máximo de advertencia.	La temperatura del servidor está aumentando.
Crítico	La temperatura ambiente de la placa del sistema está por arriba del umbral crítico máximo.	La temperatura del servidor esta aumentando demasiado.
Crítico	La corriente del seguro de corriente de la placa del sistema está fuera del límite permitido.	La corriente superó el umbral de fallas.
Crítico	Se produjo una falla en la batería de la placa del sistema.	La batería de CMOS no está presente o no tiene voltaje.
Aviso	La batería de almacenamiento tiene baja carga.	La batería de la ROMB está baja.
Crítico	Se produjo una falla en la batería de almacenamiento.	La batería de CMOS no está presente o no tiene voltaje.
Crítico	El voltaje <nombre de sensor de voltaje> de la CPU <número> superó el límite permitido.	
Crítico	El voltaje <nombre de sensor de voltaje> de la placa del sistema superó el límite permitido.	
Crítico	El voltaje <nombre de sensor de voltaje> de la tarjeta mezzanine <número> superó el límite permitido.	
Crítico	El voltaje <nombre de sensor de voltaje> del almacenamiento superó el límite permitido.	
Crítico	CPU <number> has an internal error (IERR).	Falla de la CPU.
Crítico	CPU <number> has a thermal trip (over-temperature) event.	La CPU se sobrecalentó.
Crítico	La configuración de CPU <número> no es compatible.	Tipo de procesador o ubicación incorrectos.
Crítico	CPU <número> ausente.	La CPU necesaria no se encuentra o no está presente.
Crítico	Estado de la tarjeta mezzanine B<número de ranura>: Sensor de tarjeta de complemento para la tarjeta mezzanine B<número de ranura>, se declaró un error de instalación.	Tarjeta mezzanine incorrecta instalada en la red Fabric de E/S.
Crítico	Estado de la tarjeta mezzanine C<número de ranura>: Sensor de tarjeta de complemento para la tarjeta mezzanine C<número de ranura>, se declaró un error de instalación.	Tarjeta mezzanine incorrecta instalada en la red Fabric de E/S.
Crítico	La unidad <número> se ha extraído.	La unidad de almacenamiento fue eliminada.
Crítico	Falla detectada en la unidad <número>.	Se produjo una falla en la unidad de almacenamiento.
Crítico	El voltaje a prueba de errores de la placa del sistema superó el límite permitido.	Este suceso se genera cuando los voltajes de la placa del sistema no se encuentran en los niveles normales.

Tabla 62. Pantalla de estado del servidor (continuación)

Gravedad	Mensaje	Causa
Crítico	El temporizador de vigilancia ha expirado.	El temporizador de vigilancia de iDRAC expira sin que se defina una acción.
Crítico	El temporizador de vigilancia reinició el sistema.	La vigilancia de iDRAC detectó que el sistema se bloqueó (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de reinicio.
Crítico	El temporizador de vigilancia ha apagado el sistema.	La vigilancia de iDRAC detectó que el sistema se bloqueó (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de apagado.
Crítico	El temporizador de vigilancia realizó un ciclo de encendido del sistema.	La vigilancia del iDRAC detectó que el sistema se bloqueó (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de ciclo de encendido.
Crítico	Log is full.	El dispositivo SEL (registro de sucesos del sistema) detecta que solo se podrá agregar una anotación al registro antes de que se llene.
Aviso	Se detectaron errores de memoria persistentes que se pueden corregir en un dispositivo de memoria que se encuentra en <ubicación>.	
Aviso	El porcentaje de errores persistentes que se pueden corregir aumentó en un dispositivo de memoria que se encuentra en <ubicación>.	Los errores de ECC que se pueden corregir alcanzaron un porcentaje crítico.
Crítico	Se detectaron errores de bits múltiples en un dispositivo de memoria que se encuentra en <ubicación>.	Se detectó un error de ECC incorregible.
Crítico	Se detectó un NMI de comprobación de canal de E/S en un componente del bus <número>, dispositivo <número>, función <número>.	Se generó una interrupción crítica en el canal de E/S.
Crítico	Se detectó un NMI de comprobación de canal de E/S en un componente de la ranura <número>.	Se generó una interrupción crítica en el canal de E/S.
Crítico	Se detectó un error de paridad de PCI en un componente del bus <número>, dispositivo <número>, función <número>.	Se detectó un error de paridad en el bus PCI.
Crítico	A PCI parity error was detected on a component at slot <number>.	Se detectó un error de paridad en el bus PCI.
Crítico	Se detectó un error de sistema de PCI en un componente del bus <número>, dispositivo <número>, función <número>.	El dispositivo detectó un error de PCI.
Crítico	A PCI system error was detected on a component at slot <number>. (Se ha detectado un error del sistema de PCI en un componente de la ranura <number>).	El dispositivo detectó un error de PCI.
Crítico	Se desactivó el registro de errores de memoria persistentes que se pueden corregir en un dispositivo de memoria que se encuentra en <ubicación>.	El registro de errores de un solo bit (SBE) se desactiva cuando se registran demasiados SBE en un dispositivo de memoria.
Crítico	Se ha desactivado el registro de todos los eventos.	
No es recuperable.	Se detectó un error de protocolo de CPU.	El protocolo del procesador entró en un estado que no es recuperable.
No es recuperable.	Se detectó un error de paridad en el bus de la CPU.	El PERR de bus del procesador entró en un estado que no es recuperable.
No es recuperable.	Se detectó un error de inicialización de CPU.	La inicialización del procesador entró en un estado que no es recuperable.

Tabla 62. Pantalla de estado del servidor (continuación)

Gravedad	Mensaje	Causa
No es recuperable.	Se detectó una comprobación del equipo de CPU.	La comprobación de máquina del procesador entró en un estado que no es recuperable.
Crítico	Memory redundancy is lost. (Se ha perdido la redundancia de memoria).	
Crítico	Se detectó un error fatal de bus en un componente del bus <número>, dispositivo <número>, función <número>.	Se detectó un error fatal en el bus de PCIe.
Crítico	Se detectó un NMI de software en un componente del bus <número>, dispositivo <número>, función <número>.	Se detectó un error de chip.
Crítico	No se pudo programar una dirección MAC virtual en un componente del bus <número>, dispositivo <número>, función <número>.	No se pudo programar la función FlexAddress para este dispositivo.
Crítico	Device option ROM on mezzanine card <number> failed to support Link Tuning or FlexAddress. (La ROM de opción de la tarjeta intermedia <number> no es compatible con el ajuste de vínculos o la función FlexAddress).	La ROM de opción no admite la función FlexAddress ni el ajuste de vinculación.
Crítico	No se pudieron obtener datos de iDRAC sobre ajuste de vínculos o FlexAddress.	

NOTA: Para obtener información sobre otros mensajes de LCD relacionados con el servidor, consulte "Server User Guide" (Guía del usuario del servidor).

Información de estado del servidor y del módulo de LCD

En las tablas que figuran en esta sección se describen las opciones de estado que se muestran en la pantalla LCD del panel frontal para cada tipo de componente del chasis.

Tabla 63. Estado de la CMC

Elemento	Descripción
Ejemplo: CMC1, CMC2	Nombre o ubicación.
Sin errores	Si no existen errores, aparecerá el mensaje "No errors" (Sin errores); de lo contrario, aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos de las advertencias.
Versión del firmware	Solo se muestra en las CMC activas. Indica Standby (En espera) para la CMC en espera.
IP4 <activado, desactivado>	Muestra el estado actual activado de IPv4 únicamente en un CMC activo.
Dirección IP4: <dirección, adquiriendo>	Solo se muestra si IPv4 está activado únicamente en un CMC activo.
IP6 <activado, desactivado>	Muestra el estado actual activado de IPv6 únicamente en un CMC activo.
Dirección local IP6: <dirección>	Solo se muestra si IPv6 está activado únicamente en un CMC activo.
Dirección global IP6: <dirección>	Solo se muestra si IPv6 está activado únicamente en un CMC activo.
Dirección MAC	Muestra la dirección MAC del CMC.

Tabla 64. Estado del chasis o del gabinete

Elemento	Descripción
Nombre definido por el usuario	Ejemplo: "Sistema de bastidor Dell". Puede configurar esta opción a través de la interfaz de línea de comandos (CLI) o la interfaz web de la CMC.
Mensajes de error	Si no existen errores, aparecerá el mensaje "No errors" (Sin errores); de lo contrario, aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos de las advertencias.
Número de modelo	Ejemplo: "PowerEdgeM1000e".
Consumo de alimentación	Consumo de alimentación actual en vatios.
Alimentación pico	Consumo de alimentación pico en vatios.
Alimentación mínima	Consumo mínimo de alimentación en vatios.
Temperatura ambiente	Temperatura ambiente actual en grados Celsius.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.
Modo de redundancia del CMC	No redundante o Redundante.
Modo de redundancia de la unidad de suministro de energía	No redundante, Redundancia de CA o Redundancia de CC.

Tabla 65. Estado del ventilador

Elemento	Descripción
Nombre/ Ubicación	Ejemplo: Fan1, Fan2, y así sucesivamente.
Mensajes de error	Si no se produce ningún error, aparecerá el mensaje “Sin errores”; en caso contrario se mostrará la lista con los errores críticos primero, seguidos de los avisos.
RPM	Velocidad actual del ventilador en RPM.

Tabla 66. Estado de la unidad de suministro de energía

Elemento	Descripción
Nombre/ Ubicación	Ejemplo: PSU1, PSU2, y así sucesivamente.
Mensajes de error	Si no existen errores, aparecerá el mensaje "No errors" (Sin errores); de lo contrario, aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos de las advertencias.
Estado	Desconectado, Conectado o En espera.
Potencia máxima	Potencia máxima que la unidad de suministro de energía puede proporcionar al sistema.

Tabla 67. Estado del módulo de E/S

Elemento	Descripción
Nombre/ Ubicación	Ejemplo: IOM A1, IOM B1. Y así sucesivamente.

Tabla 67. Estado del módulo de E/S (continuación)

Elemento	Descripción
Mensajes de error	Si no existen errores, aparecerá el mensaje "No errors" (Sin errores); de lo contrario, aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos de las advertencias. Para obtener más información, consulte Mensajes de error de la pantalla LCD.
Estado	Encendido o Apagado.
Modelo	Modelo del módulo de E/S.
Tipo de red Fabric	Tipo de sistema de red.
dirección IP	Solo se muestra si el módulo de E/S está encendido. En el tipo de módulo de E/S de paso el valor es cero.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.

Tabla 68. Estado de iKVM

Elemento	Descripción
Nombre	iKVM.
Sin errores	Si no existen errores, aparecerá el mensaje "No errors" (Sin errores); de lo contrario, aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos de las advertencias. Para obtener más información, consulte Mensajes de error de la pantalla LCD.
Estado	Encendido o Apagado.
Modelo/ fabricante	Descripción del modelo de iKVM.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.
Número de pieza	Número de parte del fabricante.
Versión del firmware	Versión del firmware de iKVM.
Versión del hardware	Versión de hardware de iKVM.

NOTA: Esta información se actualiza de forma dinámica.

Tabla 69. Server Status (Estado del servidor)

Elemento	Descripción
Ejemplo: Servidor 1, Servidor 2, etc.	Nombre/Ubicación.
Sin errores	Si no existen errores, aparecerá el mensaje "No errors" (Sin errores); de lo contrario, aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos de las advertencias. Para obtener más información, consulte Mensajes de error de la pantalla LCD.
Nombre de ranura	Nombre de ranura del chasis. Por ejemplo, SLOT-01. **NOTA:** Puede configurar esta tabla a través de la CLI o la interfaz web del CMC.
Nombre	Nombre del servidor, que el usuario puede establecer mediante Dell OpenManage. El nombre se muestra únicamente si la iDRAC completó el inicio y si el servidor admite esta función; en caso contrario, se muestran los mensajes de inicio de la iDRAC.
Número de modelo	Se muestra si el iDRAC completó el inicio.
Etiqueta de servicio	Se muestra si el iDRAC completó el inicio.

Tabla 69. Server Status (Estado del servidor) (continuación)

Elemento	Descripción
Versión del BIOS	Versión del firmware del BIOS del servidor.
Último código de la POST	Muestra la cadena de mensajes del último código de la POST del BIOS del servidor.
Versión del firmware del iDRAC	Se muestra si el iDRAC completó el inicio. **NOTA:** La versión de la iDRAC 1.01 se muestra como 1.1. No hay versión 1.10 de la iDRAC.
IP4 <activado, desactivado>	Muestra el estado actual activado del IPv4.
Dirección IP4: <dirección, adquiriendo>	Solo se muestra si IPv4 está activado.
IP6 <activado, desactivado>	Solo se muestra si la iDRAC admite IPv6. Muestra el estado actual activado de IPv6.
Dirección local IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
Dirección global IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
FlexAddress activado en la red Fabric	Solo se muestra si la función está instalada. Presenta las redes Fabric activadas para este servidor (es decir, A, B, C).

La información de la tabla se actualiza de forma dinámica. Si el servidor no admite esta función, la siguiente información no aparecerá; en caso contrario, las opciones de Server Administrator son las siguientes:

- Opción “Ninguna” = No se debe mostrar ninguna cadena en la pantalla LCD.
- Opción “Predeterminada” = Ningún efecto.
- Opción “Personalizada” = Permite introducir un nombre de cadena para el servidor.

La información se muestra únicamente si la iDRAC completó el inicio. Para obtener más información acerca de esta función, consulte *Chassis Management Controller for Dell PowerEdge M1000e RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para Dell PowerEdge M1000e)*, disponible en **dell.com/support/manuals**.

18

Preguntas frecuentes

En esta sección se enumeran las preguntas frecuentes para los elementos siguientes:

- RACADM
- Administración y recuperación de un sistema remoto
- Active Directory
- FlexAddress y FlexAddressPlus
- iKVM
- 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)
```

Este mensaje indica que debe emitirse otro comando solo después de que el CMC termine de reiniciarse.

Al usar subcomandos RACADM a veces se muestra uno o más de los siguientes errores:

- Mensajes de errores locales: Problemas de sintaxis, errores tipográficos, nombres incorrectos, etc. Por ejemplo: `ERROR: <message>`

Use el subcomando RACADM `help` para ver la sintaxis correcta y la información de uso.

Mensajes de error relacionados con la CMC: Problemas por los cuales la CMC no puede ejecutar una acción. También pueden decir "racadm command failed" (fallo de comando racadm).

Escriba `racadm gettracelog` para obtener información sobre la depuración.

Durante el uso del RACADM remoto, 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.

Aparece el mensaje de error "Not Found" (No se encontró) al emplear los comandos `$ logout` y `$ quit`.

Los comandos logout y quit no se admiten en la interfaz de RACADM del CMC.

Admin y recuperación de un sistema remoto

Mientras accede a la interfaz web del CMC, se muestra una advertencia de seguridad que indica que el nombre de host del certificado SSL no coincide con el nombre de host del CMC.

El CMC incluye un certificado de servidor de CMC predeterminado para garantizar la seguridad de red para las funciones de RACADM remoto e interfaz web. Cuando se utiliza este certificado, el navegador web muestra una advertencia de seguridad debido a que el

certificado predeterminado se emite al certificado predeterminado del CMC, el cual no coincide con el nombre de host del CMC (por ejemplo, la dirección IP).

Para solucionar este problema de seguridad, cargue un certificado de servidor del CMC emitido a la dirección IP del CMC. Cuando genere la solicitud de firma de certificado (CSR) que se utilizará para emitir el certificado, asegúrese de que el nombre común (CN) de la CSR coincida con la dirección IP del CMC (por ejemplo, 192.168.0.120) o el nombre DNS registrado del CMC.

Para asegurarse de que la CSR coincida con el nombre DNS registrado del CMC:

1. En la interfaz web del CMC, diríjase al árbol del sistema y haga clic en **Descripción general del chasis.**
2. Haga clic en la ficha **Red** y, a continuación, en **Red**.
   Aparecerá la página **Configuración de la red**.
3. Seleccione la opción **Registrar la CMC** en **DNS**.
4. Escriba el nombre del CMC en el campo **Nombre del CMC de DNS**.
5. Haga clic en **Aplicar cambios**.

   Para obtener más información acerca de cómo generar CSR y cómo emitir certificados, consulte Obtaining Certificates (Obtención de certificados).

   ¿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 algunos minutos en estar disponibles después de que el servidor web del CMC se restablece. El servidor web del 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 a través de la interfaz web del CMC.
   - Se cambia la propiedad **cfgRacTuneHttpsPort** (incluido cuando un comando `config -f <config file>` la cambia).
   - Se utiliza `racresetcfg` o se restablece un respaldo de la configuración del chasis.
   - Se restablece la CMC.
   - Se carga un nuevo certificado del servidor SSL.

   El servidor DNS no registra el 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.

   El CMC incluye un certificado de servidor de CMC predeterminado para garantizar la seguridad de red para las funciones de RACADM remoto e interfaz web. Este certificado no lo emite una autoridad de certificación de confianza. Para solucionar este problema de seguridad, cargue un certificado de servidor del CMC emitido por una autoridad de certificación de confianza (por ejemplo, Thawte o Verisign). Para obtener más información sobre los certificados, consulte Obtención de certificados.

   ¿Por qué se muestra el mensaje siguiente por motivos desconocidos?

   Remote Access: SNMP Authentication Failure

   Como parte del proceso de detección, 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 forma predeterminada, el nombre de comunidad para el agente del CMC es público. Cuando IT Assistant envía una solicitud de establecer, el agente del CMC genera el error de autenticación de SNMP, ya que solo acepta solicitudes de **Comunidad= público.**

   Cambie el nombre de comunidad del CMC mediante RACADM. Para establecer el nombre de comunidad del 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 autenticación de SNMP, ingrese los nombres de comunidad que acepta el agente. Dado que el CMC solo permite un nombre de comunidad, ingrese los mismos nombres de comunidad obtener y establecer para la configuración de detección 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 mismo 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 de dispositivo de RAC y el objeto de asociación) tienen que estar en el mismo dominio.

El complemento Usuarios y equipos de Active Directory extendido por Dell verifica el modo y limita a los usuarios a fin de crear objetos en varios dominios si se encuentra en modo mixto.

¿El uso del CMC con Active Directory admite varios entornos de dominio?

Sí. El nivel de la función del bosque de dominios debe estar en el modo nativo o en el modo Windows 2003. Además, los grupos entre el objeto de asociación, los objetos de usuario de RAC y los objetos de dispositivo de RAC (incluido el objeto de asociación) deben ser grupos universales.

¿Estos objetos extendidos por Dell (objeto de asociación Dell, dispositivo de RAC de Dell y objeto de privilegio Dell) pueden estar en dominios diferentes?

El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento Usuarios y equipos de Active Directory extendido por Dell permite crear estos dos objetos solamente en el mismo dominio. Los otros objetos pueden estar en diferentes dominios.

¿Existe alguna restricción para la configuración del controlador de dominio de SSL?

Sí. Todos los certificados SSL para los servidores de Active Directory del bosque deben estar firmados mediante el mismo certificado con firma de la autoridad de certificados raíz, porque la CMC solo permite cargar un certificado SSL firmado por una autoridad de certificados de confianza.

La interfaz web no se inicia una vez que se creó y se cargó un nuevo certificado RAC.

Si se utilizan los servicios de certificados de Microsoft para generar el certificado RAC, es posible que se haya utilizado la opción Certificado de usuario en lugar de Certificado web durante la creación del certificado.

Para solucionar el problema, genere una CSR, cree un certificado web nuevo utilizando los servicios de certificados de Microsoft y cárguelo mediante los siguientes comandos de RACADM:

```
racadm sslcsrgen [-g] [-f {filename}]
```

```
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress y FlexAddressPlus

¿Qué sucede si se quita una tarjeta de función?

No se producen cambios visibles si se quita una tarjeta de función. Este tipo de tarjetas pueden quitarse y almacenarse, o bien, pueden dejarse colocadas.

¿Qué sucede si se quita una tarjeta de función que se utilizó en un chasis y se coloca en otro?

La interfaz web muestra el siguiente mensaje de error:

```
This feature card was activated with a different chassis. It must be removed before accessing
the FlexAddress feature.
```

```
Current Chassis Service Tag = XXXXXXXX
```

```
Feature Card Chassis Service Tag = YYYYYYYY
```

```
An entry is added to the CMC log that states:
```

```
cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis ID='XXXXXXXX'
```

¿Qué sucede si se quita la tarjeta de función y se instala una tarjeta que no sea de FlexAddress?

No debería activarse ni se modificarse la tarjeta. La CMC no hará caso a la tarjeta. En esta situación, el comando **$racadm featurecard -s** genera el siguiente mensaje:

```
No feature card inserted
```

```
ERROR: can't open file
```

Si se reprograma la etiqueta de servicio del chasis, ¿qué sucede si hay una tarjeta de función vinculada a ese chasis?

- Si la tarjeta de función original está presente en la CMC activo en ese chasis o cualquier otro, la interfaz web mostrará el siguiente error:
  - `This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.`

- `Current Chassis Service Tag = XXXXXXXX`
- `Feature Card Chassis Service Tag = YYYYYYYY`
- La tarjeta de función original ya no se puede seleccionar para desactivarla en ese chasis ni en ningún otro, salvo que el servicio de Dell vuelva a programar la etiqueta de servicio del chasis original en un chasis y que el CMC con la tarjeta de función original se active en ese chasis.

- La función FlexAddress continúa activa en el chasis vinculado originalmente. La *vinculación* de esa función del chasis se actualiza para reflejar la nueva etiqueta de servicio.

¿Se muestra un mensaje de error si hay dos tarjetas de función instaladas en el sistema de CMC redundante?

No, no se muestra ningún mensaje de error. La tarjeta de función de la CMC activa está activa e instalada en el chasis. La CMC no hace caso a la segunda tarjeta.

¿La tarjeta SD tiene un dispositivo de protección contra escritura?

Sí. Antes de instalar la tarjeta SD en el módulo de la CMC, verifique que el seguro de protección contra escritura esté desbloqueado. La función FlexAddress no podrá activarse si la tarjeta SD está protegida contra escritura. En esta situación, el comando **$racadm feature -s** genera este mensaje:

```
No features active on the chassis. ERROR: read only file system
```

¿Qué sucede si no hay una tarjeta SD en el módulo CMC activo?

El comando **$racadm featurecard -s** muestra este mensaje:

```
No feature card inserted.
```

¿Qué le sucede a la función FlexAddress si el BIOS del servidor se actualiza de la versión 1.xx a la versión 2.xx?

Se debe apagar el módulo del servidor para poder usarlo con FlexAddress. Una vez completada la actualización del BIOS del servidor, el módulo del servidor no recibirá direcciones asignadas por el chasis hasta que se haya completado el ciclo de encendido del servidor.

¿Qué sucede si un chasis con un solo CMC se degrada con un firmware anterior a la versión 1.10?

- La función y configuración de FlexAddress se desinstalan del chasis.
- La tarjeta de función utilizada para activar la función en este chasis no se modifica y continúa vinculada al chasis. Cuando más adelante el firmware de la CMC de este chasis se actualice a la versión 1.10 u otra superior, la función FlexAddress se reactivará reinsertando la tarjeta de función original (si fuera necesario), restableciendo la CMC (si la tarjeta se insertó una vez completada la actualización del firmware) y reconfigurando la función.

¿Qué sucede si se sustituye una unidad de CMC con otra que tenga una versión de firmware inferior a 1.10 en un chasis con CMC redundantes?

En un chasis con CMC redundantes, si se está reemplazando una unidad del CMC por otra cuyo firmware es inferior a 1.10, se debe seguir este procedimiento para asegurarse de que NO se elimine la configuración y la función de FlexAddress actual:

- Asegúrese de que la versión del firmware del CMC activo sea siempre 1.10 o superior.
- Quite el CMC en espera e inserte el nuevo CMC en su lugar.
- Desde el CMC activo, actualice el firmware del CMC en espera a la versión 1.10 o superior.

NOTA: Si el firmware de la CMC en espera no se actualiza a la versión 1.10 u otra superior y ocurre una protección contra fallas, la función FlexAddress no se configura. La función debe reactivarse y reconfigurarse nuevamente.

¿Cómo se puede recuperar una tarjeta SD si no se encontraba en el chasis al ejecutar el comando de desactivación en FlexAddress?

El problema es que la tarjeta SD no puede utilizarse para instalar FlexAddress en otro chasis si no se encontraba en la CMC al momento de desactivar FlexAddress. Para recuperar el uso de la tarjeta, insértela de nuevo en una CMC del chasis con el que esté vinculada, reinstale FlexAddress y luego desactive FlexAddress nuevamente.

La tarjeta SD está instalada correctamente y se realizaron todas las actualizaciones de firmware y software. La función FlexAddress está activa, pero la pantalla de implementación del servidor no muestra las opciones para implementarla. ¿Cuál es el problema?

Este es un problema de almacenamiento en caché del navegador. Cierre el navegador y vuelva a abrirlo.

¿Qué sucede con FlexAddress si debo restablecer la configuración del chasis con el comando RACADM racresetcfg?

La función FlexAddress permanece activada y disponible. Se seleccionan de forma predeterminada todas las ranuras y redes Fabric.

NOTA: Se recomienda especialmente apagar el chasis antes de ejecutar el comando RACADM `racresetcfg`..

Después de desactivar únicamente la función FlexAddressPlus (dejando activada FlexAddress), ¿por qué falla el comando racadm setflexaddr en la CMC (aún activa)?

Si el CMC posteriormente pasa a estar activo, y la tarjeta de función FlexAddressPlus está insertada en la ranura, la función FlexAddressPlus se reactiva y es posible reanudar los cambios de la configuración de FlexAddress para ranuras y redes Fabric.

iKVM

El mensaje "User has been disabled by CMC control" (El usuario fue desactivado por el control de la CMC) aparece en el monitor conectado al panel frontal. ¿Por qué?

La CMC desactivó la conexión del panel frontal. Active el panel frontal mediante la interfaz web de la CMC o RACADM.

Para activar el panel frontal desde la interfaz web del CMC, vaya a la ficha **iKVM** > **Configuración**, seleccione la opción **Video/USB del panel frontal activado** y haga clic en **Aplicar** para guardar la configuración.

Para activar el panel frontal por medio de un comando de RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1
```

No funciona el acceso al panel posterior. ¿Por qué?

El CMC activa la configuración del panel frontal y hay un monitor conectado actualmente al panel frontal.

Solo se permite una conexión a la vez. La conexión del panel frontal tiene prioridad respecto de ACI y el panel posterior. Para obtener más información sobre la prioridad de conexión, consulte Prioridades de las conexiones del iKVM.

El mensaje "User has been disabled as another appliance is currently tiered" (El usuario fue desactivado porque otro servidor se encuentra actualmente categorizado) aparece en el monitor conectado al panel posterior. ¿Por qué?

Hay un cable de red conectado al conector del puerto ACI del iKVM y a un servidor KVM secundario.

Solo se permite una conexión a la vez. La conexión de categorización de ACI tiene prioridad respecto de la del monitor del panel posterior. El orden de prioridad es: panel frontal, ACI y panel posterior.

El indicador LED de color ámbar del iKVM está parpadeando. ¿Por qué?

Existen tres causas posibles:

- **Hay un problema con el iKVM,** por lo que debe reprogramarse. Para solucionar el problema, siga las instrucciones de actualización del firmware del iKVM.
- **El iKVM está reprogramando la interfaz de consola de la CMC.** En este caso, la consola de la CMC temporalmente no se encuentra disponible y está representada por un punto de color amarillo en la interfaz OSCAR. Este proceso lleva hasta 15 minutos.
- **El firmware del iKVM detectó un error de hardware.** Para obtener más información, consulte el estado del iKVM.

El iKVM está conectado a través del puerto ACI a un conmutador KVM externo, pero ninguna de las entradas de las conexiones de ACI está disponible.

Todos los estados muestran un punto amarillo en la interfaz OSCAR.

La conexión del panel frontal está activada y tiene un monitor conectado. Dado que el panel frontal tiene prioridad sobre el resto de las conexiones del iKVM, se desactivan los conectores de ACI y del panel posterior.

Para activar la conexión del puerto ACI, primero debe desactivar el acceso al panel frontal o quitar el monitor conectado al panel frontal. Las entradas de OSCAR del conmutador KVM externo se activarán y estarán disponibles para el acceso.

Para desactivar el panel frontal desde la interfaz web, vaya a la ficha **iKVM** > **Setup (Configuración)**, desactive la opción **Front Panel USB/Video Enabled (Video/USB del panel frontal activado)** y haga clic en Apply (Aplicar).

Para desactivar el panel frontal por medio de un comando de RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0

En el menú de OSCAR, la conexión de Dell CMC muestra una X de color rojo y no es posible conectarse a la CMC. ¿Por qué?

Existen dos causas posibles:

- **La consola de Dell CMC fue desactivada.** En este caso, para activarla puede utilizar la interfaz web de la CMC o RACADM.
- **La CMC no está disponible porque se está inicializando, se está conmutando a la CMC en espera o se está reprogramando.** En este caso, simplemente espere hasta que la CMC termine de inicializarse.

El nombre de ranura de un servidor muestra el mensaje "Initializing" (Inicializando) en OSCAR y no puede seleccionarse. ¿Por qué?

El servidor se está inicializando o el iDRAC de ese servidor sufrió una falla en el proceso de inicialización.

En principio, espere 60 segundos. Si el servidor continúa inicializándose, el nombre de ranura aparecerá en cuanto la inicialización se haya completado y podrá seleccionar el servidor.

Si después de 60 segundos OSCAR aún indica que la ranura se está inicializando, quite el servidor y vuelva a insertarlo en el chasis. Esta acción permite volver a inicializar la iDRAC.

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 icono **Refresh (Actualizar)** para ver si la dirección IP está configurada correctamente en el conmutador. Si se comete un error al configurar la dirección IP, la máscara o la 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.

Para obtener más información sobre la configuración de red del módulo de E/S, consulte los documentos *Dell PowerConnect M6220 Switch Important Information (Información importante del conmutador Dell PowerConnect M6220)* y *Dell PowerConnect 6220 Series Port Aggregator White Paper (Documento técnico sobre el agregador de puertos Dell PowerConnect serie 6220)* en **dell.com/support/manuals**.

Inicio de sesión único

Aunque el CMC está configurado para permitir un inicio de sesión único (SSO), el explorador muestra una página en blanco.

Por el momento, solo se ofrece SSO para los navegadores Mozilla Firefox e Internet Explorer. Verifique que la configuración del navegador sea correcta. Para obtener más información, consulte la sección Configuración del navegador para el inicio de sesión único.

Si los navegadores están configurados correctamente, ambos navegadores deben permitirle iniciar sesión sin introducir el nombre y la contraseña. Utilice el nombre de dominio completo (FQDN) de la CMC. Por ejemplo, escriba **myCMC.Domain.ext/** en la barra de direcciones. El navegador lo redirigirá al **https** (modo seguro) y le permitirá iniciar sesión en la CMC. Tanto **http** como **https** son válidos para los navegadores. Si guarda la URL como favorito, no deberá introducir texto después de la última barra del ejemplo. Si aún no puede iniciar sesión con SSO, consulte la sección Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en la CMC para usuarios de Active Directory.

19

Situación de uso

En esta sección se proporciona información que ayuda a navegar por secciones específicas del manual con el fin de utilizar escenarios prácticos típicos.

Temas:

Configuración básica del chasis y actualización de firmware

Este escenario lo guía para realizar las siguientes tareas:

- Dotar al chasis de configuraciones básicas.
- Verificar que el CMC detecte el hardware sin errores.
- Actualizar el firmware del CMC, los módulos de E/S y los componentes del servidor.

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

   Para obtener información sobre la instalación de un segundo CMC, consulte la sección Understanding Redundant CMC Environment (Descripción del entorno de CMC redundante).
2. Configurar el chasis con los pasos indicados en la Lista de comprobación para configurar el chasis.
3. Configurar la dirección IP de administración del CMC y la red inicial del CMC a través del panel LCD o de la consola serie del CMC Dell.

   Para obtener más información, consulte la sección Configuración inicial de red del CMC.
4. Configurar los registros y las alertas para producir registros y configurar alertas para ciertos sucesos que se producen en el sistema administrado.

   Para obtener más información, consulte la sección Configuración del CMC para enviar alertas.
5. Configurar la dirección IP y las opciones de red de los servidores que usan la interfaz web del CMC.

   Para obtener más información, consulte Configuración del servidor.
6. Configurar la dirección IP y las opciones de red de los módulos de E/S que usan la interfaz web.

   Para obtener más información, consulte la sección Configuración de los valores de red para módulos de E/S.
7. Encender los servidores.
8. Verificar los registros de hardware, los registros del CMC y las alertas de correo electrónico o de captura de SNMP para detectar configuraciones de hardware no válidas.

   Para obtener más información, consulte la sección Visualización de los registros de sucesos.
9. Para diagnosticar problemas relacionados con el hardware, acceda a la **Consola de diagnósticos**.

   Para obtener más información sobre el uso de la **Consola de diagnósticos**, consulte la sección Uso de la consola de diagnósticos.
10. Para obtener más información sobre los errores y los problemas de configuración de hardware, consulte la *Guía de referencia de mensajes de sucesos de Dell* o la *Guía de referencia de mensajes de Server Administrator*, ubicada en **dell.com/support/manuals**.
11. Actualice el firmware del CMC, los módulos de E/S y los componentes del servidor.

    Para obtener más información, consulte la sección Actualización de firmware.

Copia de seguridad de las configuraciones del CMC y de las configuraciones de servidores.

1. Para realizar una copia de seguridad de la configuración del chasis, consulte la sección Guardar o restaurar la configuración del chasis.
2. Para guardar configuraciones de un servidor, use la función **Clonación de servidores** del CMC.
   Para obtener más información consulte Configuración de las opciones de perfil con clonación de servidores.
3. Guarde las configuraciones existentes de un servidor en una tarjeta de almacenamiento externo a través de la interfaz web del CMC.
   Para obtener más información, consulte la sección Agregar o guardar perfil.
4. Aplique las configuraciones guardadas en la tarjeta de almacenamiento externo en el servidor requerido a través de la interfaz web del CMC.
   Para obtener más información, consulte la sección Aplicación de un perfil.

Actualización de firmware para consolas de administración sin inactividad de los servidores

Puede actualizar el firmware de las consolas de administración del CMC, el iDRAC y Lifecycle Controller sin inactividad en los servidores:

1. En un escenario donde tanto el CMC principal como el CMC en espera estén presentes, puede actualizar el firmware del CMC sin inactividad de los servidores o de los módulos de E/S.
2. Para actualizar el firmware en el CMC principal, consulte la sección Actualización de firmware.
   Cuando actualiza el firmware de la CMC principal, la CMC en espera se convierte en la principal. En consecuencia, no se produce inactividad en los módulos de E/S ni en los servidores.
   NOTA: El proceso de actualización del firmware afecta solo a las consolas de administración de los módulos de E/S y los servidores de la iDRAC. No afecta la conectividad externa entre los servidores y los módulos de E/S.
3. Para actualizar el firmware de la iDRAC o Lifecycle Controller sin inactividad en el chasis, realice la actualización con el servicio de Lifecycle Controller. Para obtener información sobre la actualización del firmware de los componentes de servidores mediante Lifecycle Controller, consulte la sección Actualización de firmware de los componentes de servidores.
   NOTA: Al actualizar cualquier otro componente, como tarjetas mezzanine, controladoras NDC y el BIOS, se producirá una inactividad de los servidores.

Escenarios de rendimiento de alimentación extendida: Uso de la interfaz web

Escenario 1: Cuando la función EPP se encuentra activada en una unidad de suministro de energía de 3000 W:

- Las siguientes opciones en la interfaz web se muestran atenuadas y no se pueden seleccionar:
  - Administración de la alimentación basada en servidor (SBPM).
  - Política de redundancia: Redundancia de suministro de energía y Sin redundancia.
  - Rendimiento de servidor sobre redundancia de alimentación (SPOPR).
  - Conexión dinámica de suministros de energía (DPSE).
  - Permitir operación a 110 VCA.
- Al modificar Límite de alimentación de entrada del sistema a un valor menor o igual que 13300 W, se muestra el siguiente mensaje:

```
System Input Power Cap cannot be set to less than or equal to 13300 W (45381 BTU/h) while
Extended Power Performance is enabled.
```

- Al seleccionar la casilla para activar la opción Modo de conservación máx. de alimentación (MPCM), se muestra el siguiente mensaje:

```
Enabling Max Power Conservation Mode will deactivate Extended Power Performance. Max Power
Conservation Mode option will force servers into a low power, limited performance mode and
disable server power up. Press OK to continue.
```

Escenario 2: Cuando la función EPP se encuentra desactivada en una unidad de suministro de energía de 3000 W:

- Las siguientes opciones en la interfaz web se muestran atenuadas y no se pueden seleccionar:
  - Rendimiento de servidor sobre redundancia de alimentación (SPOPR).
  - Permitir operación a 110 VCA.
- Al seleccionar la casilla para activar la opción Administración de la alimentación basada en servidor (SBPM), se muestra el siguiente mensaje:

```
Checking the Server Based Power Management Mode option will set your power cap to max
value, server priorities to default priority, and disables Max Power Conservation Mode.
Are you sure you want to continue?
```

- Al seleccionar la casilla para activar la opción Modo de conservación máx. de alimentación (MPCM), se muestra el siguiente mensaje:

```
Enabling Max Power Conservation Mode option will force servers into a low power, limited
performance mode and disable server power up. Press OK to continue.
```

Escenario 3: La opción EPP se muestra atenuada y no se puede seleccionar cuando:

- Se desactiva la función EPP en unidades de suministro de energía de 3000 W y se activa alguno de los siguientes parámetros de alimentación:
  - Administración de la alimentación basada en servidor (SBPM)
  - Política de redundancia: Redundancia de suministro de energía o Sin redundancia
  - Modo de conservación máx. de alimentación (MPCM).
  - Conexión dinámica de suministros de energía (DPSE).
  - El límite de alimentación de entrada del sistema se establece en un valor menor o igual que 13300 W (45381 BTU/h).
- El chasis no contiene seis unidades de suministro de energía de 3000 W o ninguna de las unidades de suministro de energía admite EPP, la opción EPP se muestra atenuada y no se puede seleccionar.

Escenarios de rendimiento de alimentación extendida: Uso de RACADM

Escenario 1: Administración de control de la función EPP (activar o desactivar) mediante los comandos getconfig/config set de racadm

- Para activar la función EPP en una configuración de unidad de suministro de energía de 3000 W de CA, utilice:

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

- To disable EPP feature on a 3000W AC PSU configuration, use:

```
To disable EPP feature on a 3000W AC PSU configuration, use:
```

- Para verificar si la función EPP se encuentra activada en una configuración de unidad de suministro de energía de 3000 W de CA, utilice:

```
 racadm getconfig -g cfgChassisPower -o cfgChassisEPPEnable
```

Escenario 2: Visualización del estado de la función EPP mediante `racadm getpbinfo`:

```
racadm getpbinfo
Extended Power Performance(EPP) Status = Enabled (inactive)
Available Power in EPP Pool            = 3167 W (10806 BTU/h)
Used Power in EPP Pool                 = 0 W (0 BTU/h)
EPP Percent - Available                = 100.0
```

Escenario 3: Visualización de operaciones de control de la función EPP registradas en los registros del CMC:

```
racadm getraclog
Jul 31 14:16:11 CMC-4C2WXF1 Log Cleared
Jul 31 14:15:49 CMC-4C2WXF1 Extended Power Performance is Enabled
Jul 31 14:15:49 CMC-4C2WXF1 Extended Power Performance is Disabled
```

Escenario 4: Modificación de las propiedades de configuración de la alimentación que no son compatibles con EPP, cuando la función EPP se encuentra activada:

- Activación de la administración de alimentación basada en servidor (SBMP) en una unidad de suministro de energía de 3000 W de CA

```
racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 1
This feature is not supported while Extended Power Performance is enabled.
```

- Activación de la conexión dinámica de suministros de energía en una unidad de suministro de energía de 3000 W de CA

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 1
This feature is not supported while Extended Power Performance is enabled.
```

- Cambio de la política de redundancia de alimentación de Redundancia de la red eléctrica a Redundancia de las unidades de suministro de energía en una unidad de suministro de energía de 3000 W de CA

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 2
This feature is not supported while Extended Power Performance is enabled.
```

- Cambio de la política de redundancia de alimentación de Redundancia de la red eléctrica a Sin redundancia en una unidad de suministro de energía de 3000 W de CA

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 0
This feature is not supported while Extended Power Performance is enabled.
```

- Modificación de Límite de alimentación de entrada del sistema a un valor menor o igual que 13300 W

```
racadm config -g cfgChassisPower -o  cfgChassisPowerCap 12500
System Input Power Cap cannot be set to less than or equal to  13300W (45381  BTU/h)
while Extended Power Performance is enabled.
```

- Activación de 110 VCA en una unidad de suministro de energía de 3000 W de CA

```
racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
This feature is not supported on 3000W power supplies.
```

- Activación de Modo de conservación máx. de alimentación en una unidad de suministro de energía de 3000 W de CA

NOTA: El modo de conservación máxima de alimentación (MPCM) se puede activar en una configuración de unidades de suministro de energía (PSU) de 3000 W de CA mediante la CLI de RACADM con la interfaz existente. No se produce ningún cambio en la interfaz CLI de RACADM para activar el MPCM si la función EPP se encuentra activada.

Escenario 5: Intento de activación de EPP desde una condición de inicio de desactivación mientras se establecen otros valores de configuración de la alimentación

- Activación de EPP en una unidad de suministro de energía de 3000 W de CA cuando el valor de Límite de alimentación de entrada del sistema es bajo

```
racadm config -g cfgchassispower -o cfgChassisEPPEnable
This feature is not supported while System Input Power Cap is set  to less than or equal
to 13300 W (45381 BTU/h).
```

- Activación de EPP en una unidad de suministro de energía de 3000 W de CA cuando la opción DPSE se encuentra activada

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported while Dynamic Power Supply Engagement is enabled.
```

- Activación de EPP en una unidad de suministro de energía de 3000 W de CA cuando la opción SBPM se encuentra activada

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported while Server Based Power Management is enabled.
```

- Activación de EPP en una unidad de suministro de energía de 3000 W de CA cuando la opción MPCM se encuentra activada

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported while Max Power Conservation Mode is enabled.
```

- Activación de EPP en una unidad de suministro de energía de 3000 W de CA cuando se ha establecido la política de redundancia de las unidades de suministro de energía

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported until Redundancy Policy is set to Grid Redundancy.
```

- Activación de EPP en una unidad de suministro de energía de 3000 W de CA cuando se ha establecido la política Sin redundancia

```
racadm config -g cfgChassisPower -o cfgChassisEPPEnable 1
This feature is not supported until Redundancy Policy is set to Grid Redundancy.
```

Escenario 6: Degradación de firmware cuando se activa la opción EPP en unidades de suministro de energía de 3000 W de CA

```
racadm fwupdate -g -u -a 192.168.0.100 -d firmimg.cmc -m cmc-active -m cmc-standby
Cannot update local CMC firmware: The uploaded firmware image does not support the installed
power supplies.
```