Firmware de Chassis Management Controller Dell PowerEdge M1000e

Guía del usuario versión 4.45

Notas, precauciones y avisos

NOTA: Una NOTA proporciona información importante que le ayuda a utilizar mejor su equipo.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

2013 - 08

Rev. A00

Tabla de contenido

1

Descripción general

Dell Chassis Management Controller (CMC) para el chasis Dell PowerEdge M1000e es una solución de hardware y software de administración de sistemas para administrar varios chasis de servidores de Dell. Es una tarjeta de acoplamiento activo que se instala en la parte posterior del chasis Dell PowerEdge M1000e. El CMC cuenta con microprocesador y memoria propios, y es alimentado por el chasis modular en el cual se enchufa.

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

Es posible configurar el chasis M1000e con un CMC sencillo o con CMC redundantes. En las configuraciones del CMC redundante, si el CMC principal pierde la comunicación con el chasis M1000e o la red de administración, el CMC en espera asume la administración del chasis.

El CMC proporciona varias funciones de administración de sistemas para servidores. La administración térmica y de alimentación es la función principal del CMC.

- Administración térmica y de energía automática en tiempo real de nivel de alojamiento.
  - El CMC supervisa los requisitos de alimentación del sistema y admite el modo de conexión dinámica del suministro de energía opcional. Este modo permite que el CMC mejore la eficiencia energética, al configurar las fuentes de alimentación 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.
  - El 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 alojamiento por debajo del límite de alimentación máxima definido.
  - 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.
  - El CMC comprueba la coherencia de la red Fabric de E/S entre los módulos de E/S y los servidores. Además, el 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.

Novedades de esta versión

Esta versión de CMC es compatible con:

- Habilitación de hardware para 4 bNDC Broadcom 10G KR y tarjeta mezzanine Mellanox 10G KR
- Unidades de suministro de energía de CC como opción estándar
- Bloqueo de degradación de firmware si existen suministros de energía de CC presentes
- Visualización del servidor del chasis y del inventario de componentes para el grupo de chasis
- Cambios de generación de certificados SSL únicos
- Implementación rápida de perfiles en ranuras
- Administración de configuraciones de servidores mediante perfiles: copia de seguridad, restauración, replicación. Para la replicación de perfiles de servidores, se admiten todas las configuraciones disponibles.
- Visualización de la información de la sesión de FCoE para el agregador de E/S Dell PowerEdge M1000e
- Visualización del estado de enlace ascendente y descendente del agregador de E/S Dell PowerEdge M1000e
- Compatibilidad para el modo PMUX del agregador de E/S Dell PowerEdge M1000e
- Configuración de la VLAN de administración del agregador de E/S Dell PowerEdge M1000e
- Información de apilamiento del agregador de E/S Dell PowerEdge M
- Uso de FQDN o PQDN durante la generación de certificados (en lugar del nombre único SRVTAG predeterminado del CMC existente)
- Verificación de credenciales predeterminadas y visualización de advertencias al usuario a través de la interfaz gráfica de usuario, la CLI y alertas SNMP
- Bloqueo de usuarios y direcciones IP luego de intentos de inicio de sesión incorrectos
- Inicio de iDRAC con nombre de DNS
- Compatibilidad adicional de WSMAN para OMPC
- Compatibilidad de RACADM para consultar errores activos.

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.
- 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.
- 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, unir o crear grupo y seleccionar red Fabric para arreglos de almacenamiento mediante RACADM.
- Administración de múltiples chasis:
  - capacidad de visualizar hasta ocho chasis adicionales 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.

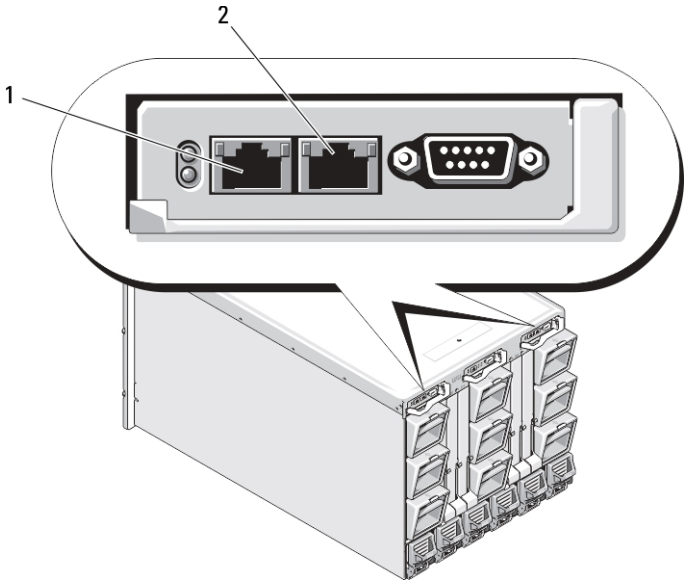
  NOTA: La interfaz web admite cifrado SSL 3.0 de 128 bits y cifrado SSL 3.0 de 40 bits (para países en los que no se admiten 128 bits).

  NOTA: Telnet no admite el cifrado SSL.
- Puertos IP configurables (si corresponde).
- Límites de errores de inicio de sesión por dirección IP, con bloqueo de inicio de sesión proveniente de la dirección IP cuando esta última ha superado el límite.

- Límite de tiempo de espera de sesión automático y configurable, y varias sesiones simultáneas.
- Rango limitado de direcciones IP para clientes que se conectan al 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.



1	Puerto GB
2	Puerto STK

Información de puertos del CMC

Se requieren los siguientes puertos TCP/IP para obtener acceso al CMC de manera remota a través de servidores de seguridad. Se trata de los puertos que el CMC utiliza para detectar las conexiones.

Tabla 1. 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 2. 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 3. 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
Power Edge 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

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

Tabla 4. 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 5. 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

Servidores	BIOS	iDRAC	Lifecycle Controller
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	6.3.0	3.50	1.6
PowerEdge M710hd	7.0.0	3.50	1.6
PowerEdge M910	2.7.9	3.50	1.6
Power Edge M915	3.0.4	3.50	1.6
PowerEdge M420	1.5.1	1.40.40	1.1.5
PowerEdge M520	1.7.4	1.40.40	1.1.5
PowerEdge M620	1.7.4	1.40.40	1.1.5
PowerEdge M820	1.5.1	1.40.40	1.1.5

NOTA: La versión 6.0.4 de Array Software admite PowerEdge PSM4110.

Conexiones de acceso remoto admitidas

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

Tabla 6. Conexiones de acceso remoto admitidas

Conexión	Características
Puertos de la interfaz de red del CMC	• Puerto GB: interfaz de red dedicada para la interfaz web del CMC; dos puertos de 10/100/1000 Mbps, uno para administración y otro para la 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.
Puerto serie	• Compatibilidad con la consola serie y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado del sistema. • Compatibilidad con intercambio binario para aplicaciones diseñadas específicamente para comunicarse mediante un protocolo binario con un tipo particular de módulo de E/S. • El puerto serie se puede conectar internamente a la consola serie de un servidor, o un módulo de E/S, mediante el comando connect (o racadm connect).

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

Plataformas admitidas

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

Para las plataformas compatibles más recientes, consulte *Léame* ubicado en **dell.com/support/manuals**.

Exploradores web admitidos

Para obtener la última información sobre los exploradores web compatibles, consulte *Léame* ubicado en **dell.com/support/manuals**.

Visualización de versiones traducidas de la interfaz web del CMC

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

1. Abra el **Panel de control** de 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

El 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 Dell Support en **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 **Elija de la lista de todos los productos Dell** y haga clic en **Continuar**. Haga clic en **Software, Supervisores, Electrónicos y Periféricos → Software**:

- Haga clic en **Remote Enterprise System Management (System Management de Remote Enterprise)** y luego haga clic en **Dell Chassis Management Controller Version 4.45** 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.
  - En la *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)* se proporciona información acerca de los subcomandos de RACADM, las interfaces admitidas y los grupos de bases de datos de propiedades y las definiciones de objetos.
  - Las *Chassis Management Controller Version 4.45 Release Notes (Notas de publicación de Chassis Management Controller versión 4.45)* proporcionan actualizaciones de última hora relativas al sistema o a la 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 número de versión necesario de iDRAC7 para ver la *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide ((Guía del usuario de Integrated Dell Remote Access Controller 7 [iDRAC7])* 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.
  - 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 notas de publicación o archivos Léame para proporcionar actualizaciones de última hora relativas al sistema o a la documentación, o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- Para obtener 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.

En ocasiones, se incluyen actualizaciones con el sistema para describir los cambios en el sistema, el software o la documentación. Lea siempre las actualizaciones primero, ya que suelen suplantar la información de otros documentos.

Cómo ponerse en contacto con Dell

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

Dell proporciona varias opciones de servicio y asistencia en línea o telefónica. Puesto que la disponibilidad varía en función del país y del producto, es posible que no pueda disponer de algunos servicios 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. Visite **dell.com/support**.
2. Seleccione la categoría de soporte.

3. Verifique su país o región en el menú desplegable Elija un país/región que aparece en la parte superior de la página.
4. Seleccione el enlace de servicio o asistencia apropiado en función de sus necesidades.

Referencia de medios sociales

Para conocer más sobre el producto, las recomendaciones e información sobre las soluciones y los servicios de Dell, puede acceder a las plataformas de medios sociales, como Dell TechCenter y YouTube. Puede acceder a blogs, foros, documentos técnicos, videos explicativos y mucho más desde la página del wiki de CMC, en **www.delltechcenter.com/cmc**. Los siguientes videos explicativos están disponibles para el CMC 4.45:

- Replicación del perfil de configuración del servidor en un chasis PowerEdge M1000E
- Asignación de perfiles a ranuras de servidores con la función de implementación rápida
- Restablecimiento de iDRAC sin reiniciar el sistema operativo
- Administración de chasis múltiples:

Estos videos explicativos también están disponibles en YouTube.

Para acceder a documentos sobre el CMC y otros documentos de firmware relacionados, visite **www.dell.com/esmmanuals**

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).

Antes de empezar

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

Además, asegúrese de tener el DVD *Dell Systems Management Tools and Documentation (Documentación y herramientas de Dell Systems Management)* que venía incluido con su sistema.

Instalación de hardware del CMC

El CMC se encuentra preinstalado en el chasis; por lo tanto, no es necesario realizar ninguna instalación. Es posible instalar un segundo CMC para que se ejecute como componente en espera para el CMC activo.

Enlaces relacionados

Descripción del entorno de CMC redundante

Lista de comprobación para configurar el chasis

Los siguientes pasos permiten configurar el chasis con precisión:

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

   NOTA: No coloque un cable en el puerto Ethernet del CMC con la etiqueta **STK**. Para obtener más información sobre el cable para el puerto STK, consulte Understanding Redundant CMC Environment (Descripción del entorno de CMC redundante).
2. Instale los módulos de E/S en el chasis y conéctelos mediante un cable.
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 lleve a cabo la configuración final del 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. Si se conectan GB y STK a la misma red (dominio de difusión) se puede producir una saturación por 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, etiquetados como **GB** (el puerto de enlace ascendente) y **STK** (el puerto de consolidación de cable o apilamiento). Con un cableado básico, puede conectar el puerto GB a la red de administración y no utilizar el puerto STK.

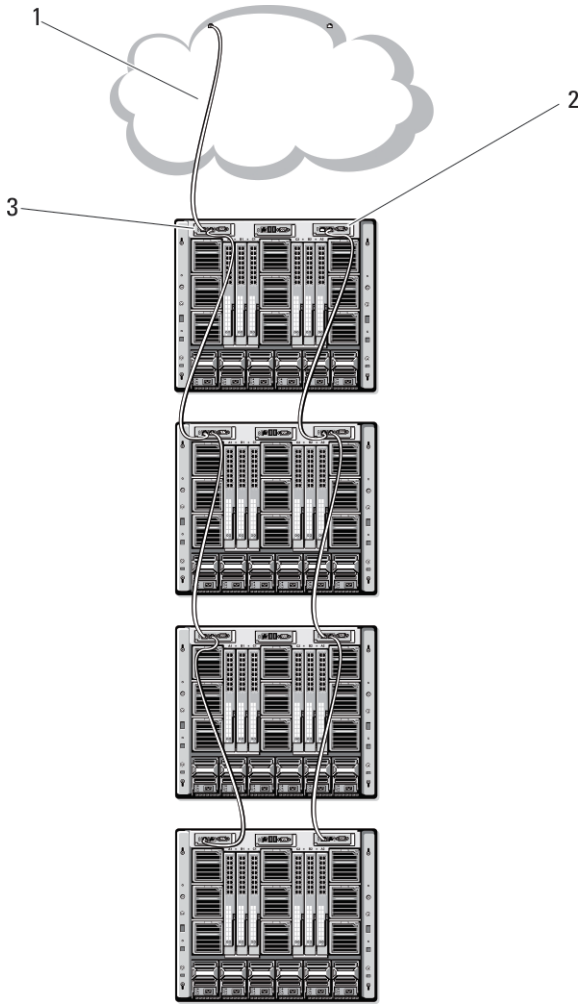
Conexión en cadena tipo margarita del CMC a la red

Si existen varios chasis en un bastidor, es posible reducir el número de conexiones a la red de administración mediante la conexión en cadena tipo margarita de hasta cuatro chasis. Si cada uno de estos cuatro chasis contiene un CMC redundante, la conexión en cadena tipo margarita permite reducir el número de conexiones a la red de administración de ocho a dos. Si los chasis solo tienen un CMC, el número de conexiones 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 el puerto STK del CMC al chasis que esté más cerca de la red. El puerto STK se debe conectar solamente a un puerto GB alejado de la cadena o la red.

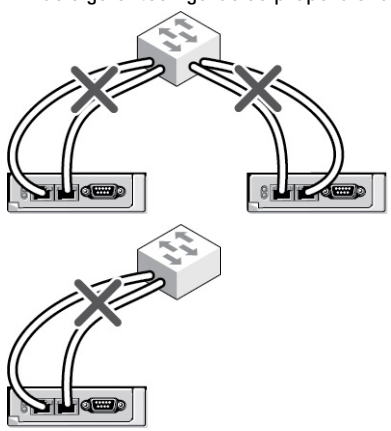
Cree cadenas separadas para los CMC en la ranura del CMC activo y en la segunda ranura del CMC.

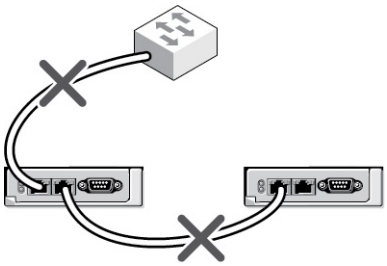
En la ilustración siguiente se muestra la organización de cables de cuatro chasis conectados en cadena radial, todos con CMC activas y en espera.



1	Red de administración
2	CMC en espera
3	CMC activo

En las siguientes figuras se proporcionan ejemplos de cableado incorrecto en el 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 interrumpir la red y provocar la pérdida de datos. La conexión de los puertos GB y STK a la misma red (dominio de difusión) puede causar una tormenta de difusión.

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

   NOTA: El restablecimiento de un CMC cuyo puerto STK está conectado en cadena a otro CMC puede interrumpir la red para los CMC que aparecen más adelante en la cadena. Los CMC subordinados podrían registrar mensajes que indiquen que se ha perdido la conexión con la red y podrían desactivarse y ceder sus funciones a los 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 el RACADM remoto desde la estación de administración, instale el RACADM remoto por medio del DVD *Dell Systems Management Tools and Documentation (Documentación y herramientas de Dell Systems Management)* que está disponible con el sistema. Este DVD incluye los siguientes componentes de Dell OpenManage:

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

Para obtener información sobre la instalación de los componentes de software de Dell OpenManage, consulte *Dell OpenManage Installation and Security User's Guide (Guía del usuario de instalación y seguridad de Dell OpenManage)* disponible en el DVD o en **dell.com/support/manuals**. También puede descargar la última versión de las herramientas Dell DRAC Tools de **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 mediante la opción `–noexec mount`. Esta opción no permite ejecutar ningún archivo ejecutable desde el DVD. Es necesario montar el DVD-ROM manualmente y, a continuación, ejecutar los archivos ejecutables.
4. Desplácese hasta el directorio **SYSMGMT/ManagementStation/linux/rac**. Para instalar el software RAC, escriba el siguiente comando:

   ```
   rpm –ivh *.rpm
   ```
5. Para obtener ayuda sobre el comando RACADM, escriba `racadm help` después de ejecutar los comandos anteriores. Para obtener más información sobre RACADM, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

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

Configuración de un explorador web

Puede configurar y administrar el CMC, los servidores y los módulos instalados en el chasis por medio del explorador web. Consulte la sección *Exploradores compatibles* en *Léame* en **dell.com/support/manuals**.

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

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

Enlaces relacionados

Servidor proxy
Filtro de suplantación de identidad de Microsoft
Obtención de la lista de revocación de certificados
Descarga de archivos desde el CMC con Internet Explorer

Activación de animaciones en Internet Explorer

Servidor proxy

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

Internet Explorer

Para editar la lista de excepciones en Internet Explorer:

1. Inicie Internet Explorer.
2. Haga clic en **Herramientas** → **Opciones de Internet** → **Conexiones**.
3. En la sección **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.
   Aparecerá el cuadro de diálogo **Configuración de la red de área local (LAN)**.
4. En el cuadro de diálogo **Configuración de la red de área local (LAN)**, diríjase a la sección **Servidor proxy**. Seleccione la opción **Usar un servidor proxy para la LAN**.
   Se activará la opción **Avanzado**.
5. Haga clic en **Avanzado**.
6. En la sección **Excepciones**, agregue las direcciones para los CMC y los iDRAC de la red de administración en la lista de valores separados por punto y coma. Es posible usar nombres DNS y comodines en las anotaciones.

Mozilla Firefox

Para editar la lista de excepciones en Mozilla Firefox versión 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 usar proxy para**, escriba las direcciones para los CMC y los iDRAC de la red de administración como lista de valores separados por comas. Es posible usar nombres DNS y comodines en las anotaciones.

Filtro de suplantación de identidad de Microsoft

Si se activa el filtro de suplantación de identidad (phishing) de Microsoft en Internet Explorer 7 en el sistema de administración y el CMC no tiene acceso a Internet, el acceso al CMC puede demorarse unos segundos. Esta demora puede ocurrir si se utiliza el explorador u otra interfaz como RACADM remoto. Realice 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 el CMC no dispone de un 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 Web Server del CMC utiliza un certificado incluido en la lista de certificados revocados que se recupera de Internet. Si no es posible obtener acceso a Internet, esta función puede generar una demora de varios segundos cuando se obtiene acceso al CMC mediante el explorador o con una interfaz de línea de comandos como el RACADM remoto.

Para desactivar la obtención de la CRL:

1. Inicie Internet Explorer.
2. Haga clic en **Herramientas** → **Opciones de Internet** y, a continuación, haga clic 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 **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 mostrar 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 la configuración de los valores de red del CMC, consulte Configuring Initial CMC Network (Configuración inicial de red del CMC). Esta configuración inicial asigna los parámetros de red TCP/IP que permiten obtener acceso al CMC.

Asegúrese de que el CMC y el iDRAC en 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.

El CMC se conecta a la red de administración. Todo el acceso externo al CMC y a los iDRAC se realiza mediante el CMC. Recíprocamente, el acceso a los servidores administrados se realiza mediante conexiones de red a los módulos de E/S. 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 admitir ni garantizar el tiempo activo de 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 entre el CMC y el iDRAC. Estas demoras pueden provocar un comportamiento impredecible en el chasis, por ejemplo, que el CMC muestre al iDRAC como fuera de línea aunque esté encendido y en funcionamiento, lo que a su vez genera otros comportamientos no deseados. Si no es práctico aislar físicamente la red de administración, la otra opción es enviar el tráfico del CMC y del iDRAC a una red VLAN separada. Las interfaces de red del iDRAC individual y del CMC pueden configurarse para usar una red VLAN.

Si existe un chasis, conecte el CMC y el CMC en espera a la red de administración. Si existe un CMC redundante, use otro cable de red y conecte el puerto **GB** del CMC a un segundo puerto de la red de administración.

Si existe más de un chasis, es posible elegir entre una conexión básica, donde cada CMC se conecta a la red de administración, o una conexión de chasis en cadena tipo margarita, donde el chasis se conecta en serie y solamente un 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 tipo margarita utiliza menos puertos en la red de administración, pero introduce dependencias entre los CMC, lo que 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.

Enlaces relacionados

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

Configuración inicial de red del CMC

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

La configuración inicial de red del CMC se puede realizar antes o después de asignar una dirección IP al CMC. Para configurar las opciones iniciales de red del CMC antes de tener una dirección IP, se 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

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

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

NOTA: La opción de configurara el CMC con el panel LCD está disponible solamente hasta que se implementa el CMC o hasta que se cambia la contraseña predeterminada. Si no se cambia la contraseña, puede seguir usando el LCD para restablecer las configuraciones del CMC, lo que causará un posible riesgo de seguridad.

El panel LCD se encuentra en la esquina inferior izquierda en el frente 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 mientras se enciende. Cuando está lista, se muestra la pantalla **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 **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.

   Para que el rendimiento de la red sea eficaz, el valor de Velocidad de la red debe coincidir con la configuración de la red. Si asigna a Velocidad de la red un valor menor que la velocidad de la configuración de la red, el consumo de ancho de banda aumenta y la comunicación por medio de la red se vuelve más lenta. **Determine si la red es compatible con las velocidades de red anteriores y defina el valor según corresponda.** Si la configuración de la red no coincide con ninguno de estos valores, se recomienda usar la Negociación automática (opción **Automática**) o consultar al fabricante del equipo 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)	El CMC recupera la configuración IP (dirección IP, máscara y puerta de enlace) automáticamente de un servidor DHCP en la red. Se asigna una dirección IP exclusiva al CMC que se distribuye a través de la red. Si ha seleccionado la opción DHCP, presione el botón central. Aparecerá la pantalla **Configurar iDRAC7**; 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:

- Establezca el valor de **Dirección IP estática** con las teclas de flecha hacia la derecha o hacia la izquierda para moverse entre las posiciones, y las teclas de flecha hacia arriba y hacia abajo para seleccionar un número para cada posición. Cuando haya terminado de configurar **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 **Resumen de la red**.

  La pantalla **Resumen de la red** muestra los valores de **Dirección IP estática**, **Máscara de subred** y **Puerta de enlace** que ha introducido. Compruebe que los valores sean correctos. Para corregir un valor, vaya al botón de flecha hacia la izquierda y presione la tecla central para regresar a la pantalla de ese valor. Después de hacer una corrección, presione el botón central.
- Cuando haya confirmado que los valores introducidos son correctos, presione el botón central. Aparecerá la pantalla **¿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.

   Para 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 **¿Registrar DNS?**; vaya al paso 10.

   Establezca el valor de **Dirección IP de DNS** con las teclas de flecha hacia la derecha o hacia la izquierda para moverse entre las posiciones, y las teclas de flecha hacia arriba y hacia abajo para seleccionar un número para 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)	El iDRAC recupera la configuración IP (dirección IP, máscara y puerta de enlace) automáticamente de un servidor DHCP en la red. Se asigna una dirección IP exclusiva al iDRAC que se distribuye a través de 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: – Establezca el valor de **Dirección IP estática** con las teclas de flecha hacia la derecha o hacia la izquierda para moverse entre las posiciones, y las teclas de flecha hacia arriba y hacia abajo para seleccionar un número para cada posición. Esta dirección es la IP estática del iDRAC que se encuentra en la primera ranura. La dirección IP estática de cada iDRAC posterior se calcula como un incremento de número de la ranura de esta dirección IP. Cuando haya terminado de configurar **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 si desea **Activar** o **Desactivar** el canal de LAN de IPMI. Presione el botón central para continuar.
- En la pantalla **Configuración del iDRAC**, seleccione el icono **Aceptar/Sí** y presione el botón central para aplicar toda la configuración de red del iDRAC a los servidores instalados. Para no aplicar los ajustes de red del iDRAC a los servidores instalados, seleccione el icono **No**, oprima el botón central y continúe con el paso c.
- En la siguiente pantalla de **Configuración del iDRAC**, seleccione el icono Aceptar/Sí y presione el botón central para aplicar toda la configuración de red del iDRAC a los servidores recién instalados; cuando se inserte un servidor nuevo en el chasis, la pantalla LCD le preguntará al usuario si desea implementar automáticamente el servidor con las políticas o los valores de red configurados previamente. Para no aplicar la configuración de red del iDRAC a 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 del iDRAC.

11. En la pantalla **Gabinete**, seleccione el icono **Aceptar/Sí** y presione el botón central para aplicar toda la configuración del gabinete. Para no aplicar la configuración del gabinete, seleccione el icono **No** y presione el botón central.
12. En la pantalla **Resumen de IP**, revise las direcciones IP que proporcionó para asegurarse de que sean correctas. Para corregir un valor, vaya al botón de flecha hacia la izquierda y presione la tecla central para regresar a la pantalla de ese valor. Después de hacer una 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 **Resumen de IP**.

    Después de confirmar que los valores que introdujo son correctos, presione el botón central. El asistente de configuración se cerrará y regresará a la pantalla **Menú principal**.

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

    El CMC y los iDRAC ahora están disponibles en la red. Puede obtener acceso al CMC en la dirección IP asignada por medio de la interfaz web o las interfaces de línea de comandos, por ejemplo, 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 configurados los valores de red del CMC, es posible obtener acceso al CMC de manera remota por medio de diversas interfaces. En la siguiente tabla se enumeran las interfaces que se pueden utilizar para obtener acceso al CMC de manera remota.

NOTA: Ya que Telnet no ofrece tanta seguridad como las otras interfaces, esa opción está desactivada de manera predeterminada. Para activar Telnet, se puede utilizar la Web, SSH o el RACADM remoto.

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

Tabla 7. Interfaces del CMC

Interfaz	Descripción
Interfaz web	Proporciona acceso remoto al CMC por medio de una interfaz gráfica de usuario. La interfaz web está incorporada en el firmware del CMC y se puede obtener

Interfaz	Descripción
	acceso a ella por medio de la interfaz del NIC desde un explorador web compatible en la estación de administración. Para obtener una lista de los exploradores web compatibles, consulte la sección correspondiente en *Léame* 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 trabajo. Utiliza la interfaz de red fuera de banda para ejecutar los comandos RACADM en los sistemas administrados y utiliza el canal HTTPS. La opción `-r` ejecuta el comando RACADM sobre una red. • Se puede obtener acceso al RACADM de firmware cuando se inicia sesión en el CMC mediante SSH o Telnet. Es posible ejecutar los comandos de RACADM de firmware sin especificar el nombre de usuario, la contraseña o la dirección IP del CMC. Después de introducir los valores necesarios en la petición de RACADM, es posible 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. Para restablecer el CMC sin reiniciar el servidor, mantenga presionado el botón Identificación del sistema durante 16 segundos.
Telnet	Proporciona acceso de la línea de comandos al CMC a través de la red. La interfaz de línea de comandos RACADM y el comando connect, que se utiliza para conectar a la consola serie de un servidor o módulo de E/S, están disponibles desde la línea de comandos del CMC. **NOTA:** Telnet no es un protocolo seguro y está desactivado de manera predeterminada. Telnet 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. Esto proporciona las mismas capacidades que la consola Telnet, pero utiliza una capa de transporte cifrada para aumentar la seguridad. El servicio SSH está activado de forma predeterminada en el CMC y se puede desactivar.
WS-MAN	Los servicios remotos LC se basan en el protocolo WS-Management para realizar tareas de administración de uno a varios sistemas. Debe utilizar el cliente WS-MAN como cliente WinRM (Windows) o cliente OpenWSMAN (Linux) para utilizar la funcionalidad Servicios remotos LC. También puede utilizar Power Shell y Python para crear secuencias de comandos para la interfaz WS-MAN. 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. El CMC usa WS–Management para transmitir información de administración basada en el modelo común de información (CIM) para el grupo de trabajo de administración distribuida (DMTAF). La información CIM define la

Interfaz	Descripción
	semántica y los tipos de datos que se pueden modificar en un sistema administrado. La implementación WS-MAN del CMC usa SSL en el puerto 443 para la seguridad de transporte y admite la autentificación básica. Los datos disponibles a través de WS-Management se proporcionan con la interfaz de instrumentación del CMC asignada a los perfiles de DMTF y los perfiles de extensión. Para obtener más información, 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 WS-MAN. • **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 del CMC mediante Dell Server Administrator, ejecute Server Administrator en la estación de administración. En el árbol del sistema que se encuentra en el panel de la izquierda de la página de inicio de Server Administrator, haga clic en **Sistema** → **Chasis del sistema principal** → **Remote Access Controller**. Para obtener más información, consulte *Dell Server Administrator User's Guide (Guía del usuario de Dell 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 Ubicación del chasis es opcional. Se recomienda usar los campos **Centro de datos**, **Pasillo**, **Bastidor** y **Ranura de bastidor** para indicar la ubicación física del chasis.
3. Haga clic en **Aplicar**. Se guardará la configuración.

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

Para establecer la ubicación o el nombre del chasis, así como la fecha y la hora, mediante la interfaz de línea de comandos, consulte los comandos **setsysinfo** y **setchassisname**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*.

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 Descripción general del chasis y haga clic en **Configuración** → **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 mediante la interfaz de línea de comandos, consulte las secciones del comando config y del grupo de propiedades de la base de datos `cfgRemoteHosts` en *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*.

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 <módulo> [-l <estadoLed>]
```

donde *<módulo>* especifica el módulo cuyo LED desea configurar. Las opciones de configuración son:

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

y *<estadoLed>* 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 del CMC con RACADM, utilice el subcomando `cfgRacTuneIdracDNSLaunchEnable`. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de línea de comandos RACADM para iDRAC7 y CMC)*.

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**.

La **Seguridad de inicio de sesión** le permite configurar los atributos de rango de IP para el inicio de sesión en el CMC con la interfaz web del 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**. De manera alternativa, para acceder a la página **Seguridad de inicio de sesión**, en el árbol del sistema, en **Descripción general del chasis**, haga clic en **Seguridad** → **Inicio de sesión**.

   Aparecerá la página **Seguridad de inicio de sesión**.
3. Para activar la función de bloqueo de usuarios o bloqueo de IP, en la sección **Política de bloqueo de inicio de sesión**, seleccione **Bloqueo por nombre de usuario** o **Bloqueo por dirección IP (IPV4)**.

   Se activarán las opciones para configurar los otros atributos de la política de bloqueo de inicio de sesión.
4. Introduzca los valores requeridos de los atributos de la política de bloqueo de inicio de sesión en los campos activados: **Bloqueo por conteo de intentos fallidos**, **Ventana de bloqueo por intentos fallidos** y **Bloqueo por tiempo de penalidad**. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el 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 sobre estos objetos, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*, disponible en **dell.com/support/manuals**.

Descripción del entorno de CMC redundante

Es posible instalar un CMC en espera que tome el control si el CMC activo falla. El CMC redundante puede estar preinstalado o agregarse posteriormente. Es importante que la red del CMC esté correctamente conectada para garantizar una redundancia total y un rendimiento óptimo.

Las protecciones contra fallas pueden ocurrir cuando:

- Ejecuta el comando **cmcchangeover** de RACADM. (Consulte la sección del comando **cmcchangeover** en *RACADM Command Line Reference Guide for iDRAC7 and CMC [Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC])*.
- Ejecuta el comando racreset de RACADM en el CMC activo. (Consulte la sección del comando **racreset** en *RACADM Command Line Reference Guide for iDRAC6 and CMC [Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC])*.
- Restablece el CMC activo desde la interfaz web. (Consulte la opción **Restablecer el CMC** para el contenido **Operaciones de control de alimentación** que se describe en Executing Power Control Operations [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 el CMC, se perderán todas las conexiones del iDRAC y todas las sesiones activas del CMC. Los usuarios que hayan perdido su sesión deberán volver a conectarse al nuevo CMC activo.

Enlaces relacionados

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

Acerca del CMC en espera

El CMC en espera es idéntico al CMC activo y se mantiene como un reflejo de ese CMC. Los CMC activo y en espera deben tener instalada la misma revisión de firmware. Si las revisiones de firmware son diferentes, el sistema informará que existe una redundancia degradada.

El CMC en espera asume las mismas propiedades y configuración del CMC activo. Se debe mantener la misma versión de firmware en ambos CMC, pero no es necesario duplicar los valores de configuración en el CMC en espera.

NOTA: Para obtener información acerca de la instalación de un CMC en espera, consulte *Hardware Owner's Manual (Manual del propietario de hardware)*. Para obtener instrucciones sobre la instalación del firmware de CMC en el CMC en espera, siga las instrucciones descritas en Updating Firmware (Actualización de firmware).

Modo a prueba de fallos de CMC

En el modo a prueba de fallos, similar a la protección contra fallas que ofrece el CMC redundante, el gabinete M1000e activa este modo para proteger los sistemas blade y los módulos de E/S de posibles fallos. El modo a prueba de fallos se activa cuando no existe ningún CMC controlando el chasis. Durante el período de protección contra fallas de un CMC o durante una pérdida de administración de un CMC sencillo:

- 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 del CMC o pérdida de la conexión de red: la administración del chasis se reanuda después de que el chasis cede el control al CMC en espera después de una falla. La protección contra fallas de la red solo está activada 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 de firmware 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. Se recomienda actualizar primero el CMC en espera, de manera que se produzca un solo suceso de protección contra fallas.
- 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 del CMC; es decir, la ranura no indica la prioridad. En lugar de eso, el CMC que se instala o se inicia primero asume la función del CMC activo. Si se aplica corriente alterna con dos CMC instalados, el CMC instalado en la ranura 1 del chasis del CMC (la izquierda) generalmente se convierte en el CMC activo. El CMC activo se indica con el LED azul.

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

Obtención del estado de condición del CMC redundante

Es posible ver el estado de condición del CMC en espera en la interfaz web. Para obtener más información sobre el acceso al estado de condición del CMC en la interfaz web, consulte Viewing Chassis Information and Monitoring Chassis and Component Health (Visualización de información del chasis y supervisión de la condición de los componentes y del chasis).

3

Inicio de sesión en el CMC

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

Enlaces relacionados

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

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 obtener acceso al CMC mediante la dirección IPv4: `https://<Dirección IP de CMC>`

     Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://<Dirección IP de CMC>:<Número de puerto>`
   - Para obtener acceso al CMC mediante la dirección IPv6: `https://[<Dirección IP de CMC>]`

     Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://[<Dirección IP de CMC>]:<Número de puerto>`

     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.

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

Enlaces relacionados

Configuración de un explorador web
Inicio de sesión en CMC como usuario local, usuario de Active Directory o usuario LDAP
Inicio de sesión en el CMC mediante una tarjeta inteligente

Inicio de sesión en el CMC mediante inicio de sesión único

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

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

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

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.

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

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

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

   NOTA: Este campo distingue entre mayúsculas y minúsculas.
3. De forma opcional, seleccione un límite de tiempo de espera para la sesión. El tiempo de espera es el período durante el cual puede permanecer conectado sin actividad antes de que el sistema cierre la sesión automáticamente. El valor predeterminado es el tiempo de espera en inactividad de los servicios web.
4. Haga clic en **Aceptar**.

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

Enlaces relacionados

Configuración de cuentas de usuario y privilegios
Acceso a la interfaz web del CMC

Inicio de sesión en el CMC mediante una tarjeta inteligente

Es posible iniciar sesión en el CMC mediante una tarjeta inteligente. Las tarjetas inteligentes proporcionan una autentificación de factor doble (TFA) y ofrecen dos niveles de seguridad:

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

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

NOTA: No se puede utilizar la dirección IP para iniciar sesión en el CMC con el inicio de sesión mediante 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 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 el CMC mediante el vínculo `https://<nombredecmc.nombre-dominio>`.

   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 del CMC mediante `<nombredecmc.nombre-dominio>:<número de puerto>`, donde nombredecmc es el nombre de host del CMC, **nombre-dominio** es el nombre del dominio y **número de puerto** 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 el CMC mediante las credenciales de Active Directory.

Enlaces relacionados

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

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 se puede utilizar la dirección IP para obtener acceso al inicio de sesión único. Kerberos valida las credenciales en función del nombre de dominio completo (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 su cuenta de red.
2. Obtenga acceso a la interfaz web del CMC mediante: `https://<nombredecmc.nombre-dominio>`.

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

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

El CMC lo conectará utilizando las credenciales Kerberos que el explorador almacenó en caché cuando inició sesión utilizando su cuenta de Active Directory válida. Si la conexión falla, el explorador se desvía a la página de inicio de sesión normal del 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.

Enlaces relacionados

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

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.

Enlaces relacionados

Configuración del CMC para el uso de consolas de línea de comandos
Activación del acceso al iKVM desde Dell CMC Console

Acceso al CMC mediante RACADM

RACADM proporciona un conjunto de comandos que permiten configurar y administrar el CMC mediante una interfaz de texto. Es posible obtener acceso 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:

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

- 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 el 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 del CMC.

Es posible utilizar comandos de RACADM remoto en secuencias de comandos para configurar varios CMC. El CMC no admite secuencias de comandos, por lo que no se pueden ejecutar secuencias de comandos directamente en el CMC.

Para obtener más información sobre RACADM, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

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

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

Es posible iniciar sesión en el CMC a través de SSH sin introducir ninguna contraseña. También se puede enviar un único comando RACADM como un 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**: `servicio ssh@<dominio>` o `servicio ssh@<dirección_IP>` donde dirección_IP es la dirección IP del CMC.
- **Envío de comandos RACADM**: `servicio ssh@<dominio> racadm getversion` y `servicio ssh@<dominio> 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. 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.

Enlaces relacionados

Configuración de la autentificación de clave pública en SSH

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 8. Varias sesiones en el CMC

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

Cambio de la contraseña de inicio de sesión predeterminada

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

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

Se muestra el mismo mensaje de advertencia si inicia sesión con Active Directory o LDAP. Las cuentas de Active Directory y LDAP no se tienen en cuenta al momento de determinar si alguna cuenta (local) tiene `root` y `calvin`

como credenciales. También aparece un mensaje de advertencia al iniciar sesión en el CMC con SSH, Telnet, RACADM remoto o la interfaz web. Para la interfaz web, SSH y Telnet, se muestra un solo mensaje de advertencia para cada sesión. Para RACADM remoto, se muestra el mensaje de advertencia para cada comando.

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

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

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

Cuando se conecta a la interfaz web del CMC, si aparece la página **Advertencia de contraseña predeterminada**, puede cambiar la contraseña. Para ello, haga lo siguiente::

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: +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, I, \
3. En el campo **Confirmar contraseña**, escriba nuevamente la contraseña.
4. Haga clic en **Continuar**. Se configura la contraseña nueva y queda conectado al 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>` (<índice>) es un valor de 1 a 16 (indica la cuenta de usuario) y `<newpassword>` (<nueva_contraseña>) es la contraseña nueva definida por el usuario.

Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC).

Activación o desactivación del mensaje de advertencia de contraseña predeterminada

Es posible activar o desactivar el mensaje de advertencia de contraseña predeterminada. Para hacerlo, se 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 **Advertencia de contraseña predeterminada**, seleccione **Activar** y, a continuación, haga clic en **Aplicar** para activar la visualización de la página **Advertencia de contraseña predeterminada** cuando inicie sesión en el CMC. De lo contrario, seleccione **Desactivar**.

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

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

Para activar la visualización del mensaje de advertencia y cambiar la contraseña de inicio de sesión predeterminada con RACADM, use el objeto `racadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> o <1>`. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*, 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: los iDRAC anteriores al iDRAC6 se deben actualizar mediante la interfaz de recuperación. El firmware del iDRAC6 también se puede actualizar con la interfaz de recuperación, pero es obsoleto para el iDRAC6 y las versiones futuras.
- BIOS
- Unified Server Configurator
- Diagnósticos de 32 bits
- Driver Pack del SO
- Controladoras de interfaz de red
- Controladoras RAID

Enlaces relacionados

Descarga de firmware del CMC
Visualización de versiones de firmware actualmente instaladas
Actualización de firmware del CMC
Actualización de firmware del iKVM
Actualización de firmware del iDRAC del servidor
Actualización de firmware de los componentes del servidor
Recuperación de firmware del iDRAC mediante el CMC
Actualización de firmware de los dispositivos de infraestructura de módulo de E/S

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

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**
- **Descripción general del chasis → Descripción general del módulo de E/S → 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 actualmente instaladas mediante RACADM, use el subcomando **getkvminfo**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

Actualización de firmware del CMC

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

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

Si se utiliza una sesión de interfaz de usuario web para actualizar el firmware de los componentes del sistema, se debe establecer un valor suficientemente elevado en Tiempo de espera en inactividad para adecuarse al tiempo de transferencia de archivos. En algunos casos, es posible que el tiempo de transferencia de archivos de firmware sea de hasta 30 minutos. Para configurar el valor de Tiempo de espera en inactividad, consulte Configuring Services (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 existen CMC redundantes instalados en el chasis, se recomienda actualizar los dos CMC a la misma versión de firmware al mismo tiempo con una sola operación. Si el firmware de los CMC es diferente y se produce una protección contra fallas, se pueden producir resultados inesperados.

Una vez cargado correctamente el firmware, el CMC activo se restablecerá y no estará disponible temporalmente. Si existe un CMC en espera, las funciones de ambos CMC se intercambiarán. El CMC en espera se convertirá en el CMC activo. Si se aplica una actualización solamente al CMC activo, una vez completado el restablecimiento, el CMC activo no ejecutará la imagen actualizada, solo el CMC en espera tendrá esa imagen. Como regla general, se recomienda especialmente mantener versiones de firmware idénticas para el CMC activo y el CMC en espera.

Cuando haya actualizado el CMC en espera, intercambie las funciones de los CMC para que el CMC recientemente actualizado se convierta en el CMC activo y el CMC con la versión de firmware más antigua se convierta en el CMC en

espera. Consulte la sección del comando `cmcchangeover` en *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC) para obtener

información sobre el intercambio de funciones. Esto le permitirá verificar que la actualización se haya realizado correctamente y que el nuevo firmware funcione apropiadamente, antes de actualizar el firmware en el segundo CMC. Cuando ambos CMC se encuentren actualizados, podrá usar el comando `cmcchangeover` para restaurar los CMC a sus funciones anteriores. La revisión de firmware 2.x del CMC actualiza tanto el CMC principal como el CMC redundante sin usar el comando `cmcchangeover`.

Para evitar la desconexión de otros usuarios durante el restablecimiento, informe sobre este proceso a los usuarios autorizados con posibilidades de conectarse al CMC y compruebe si existen sesiones activas en la página Sesiones. Para abrir la página **Sesiones**, seleccione **Chasis** en el árbol, haga clic en la ficha **Red** y haga clic en la subficha **Sesiones**.

Al transferir archivos hacia y desde el CMC, el icono de transferencia de archivos gira durante la transferencia. Si el icono está animado, asegúrese de que el explorador esté configurado para permitir animaciones. Para obtener instrucciones, consulte Allow Animations in Internet Explorer (Habilitación de animaciones en Internet Explorer).

Si experimenta problemas al descargar archivos desde el CMC mediante Internet Explorer, active la opción No guardar páginas cifradas en el disco. Para obtener instrucciones, consulte Downloading Files From CMC With Internet Explorer (Descarga de archivos desde el CMC con Internet Explorer).

Enlaces relacionados

Descarga de firmware del CMC

Visualización de versiones de firmware actualmente instaladas

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**
   - **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**.
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 **Imagen del firmware**, introduzca la ruta de acceso del archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para dirigirse a la ubicación del archivo. El nombre predeterminado de la imagen del firmware del CMC es `firmimg.cmc`.
4. Haga clic en **Iniciar actualización del firmware** y seleccione **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 un CMC en espera, el campo **Estado de la actualización** mostrará el mensaje **Listo** cuando se complete la actualización. En un CMC activo, durante las etapas finales del proceso de actualización de firmware, la sesión del explorador y la conexión con el CMC se perderán temporalmente debido a la desconexión del CMC activo. Cuando el CMC activo se reinicie, deberá volver a iniciar sesión después de unos minutos. Después de que el CMC se reinicie, se mostrará el nuevo firmware en la página **Actualización del firmware**.

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

Actualización de firmware del CMC mediante RACADM

Para actualizar el firmware del CMC mediante RACADM, utilice el subcomando `fwupdate`. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de línea de comandos RACADM para iDRAC7 y CMC)*.

Actualización de firmware del iKVM

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

Enlaces relacionados

Descarga de firmware del CMC

Visualización de versiones de firmware actualmente instaladas

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**, active la casilla de la columna **Actualizar destinos** para el **iKVM** cuyo firmware desea actualizar y haga clic en **Aplicar actualización de iKVM**.
3. En el campo **Imagen del firmware**, introduzca la ruta de acceso del archivo de imagen del firmware en la estación de administración o en la red compartida, o bien, haga clic en **Examinar** para dirigirse a la ubicación del archivo. El nombre predeterminado de la imagen del firmware del 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 *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de línea de comandos RACADM para iDRAC7 y CMC)*.

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

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

El CMC solamente permite las actualizaciones de firmware de dispositivos de infraestructura de módulo de E/S (IOMINF) si detecta que el firmware de IOMINF está desactualizado con respecto a la imagen almacenada en el sistema de archivos del CMC. Si el firmware de IOMINF está actualizado, el CMC evita las actualizaciones de IOMINF. Los dispositivos IOMINF actualizados no se incluyen en la lista de dispositivos actualizables.

Enlaces relacionados

Descarga de firmware del CMC
Visualización de versiones de firmware actualmente instaladas
Actualización de software de módulo de E/S mediante la interfaz web del CMC

Actualización de firmware de 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**
   Aparecerá la página **Firmware y software de 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 **Firmware y software de módulo de E/S**.

2. En la página **Firmware y software de módulo de E/S**, dentro de la sección **Firmware de E/S**, seleccione la columna **Actualizar** para el módulo de E/S para el que desea actualizar el software y haga clic en **Aplicar actualización de software**.

   La sección **Estado de actualización** 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: 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, 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**.

Actualización de firmware de módulo de E/S mediante RACADM

Para actualizar el firmware de los dispositivos de infraestructura de módulo E/S, utilice el subcomando fwupdate. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

Actualización de firmware del iDRAC del servidor

Es posible actualizar el firmware para el iDRAC6 y el iDRAC7.

El firmware del iDRAC debe ser de una versión 1.4 o superior para los servidores con iDRAC, o 2.0 o superior para los servidores con iDRAC6 Enterprise. Si se desea actualizar el firmware del iDRAC a una versión 3.0 o superior desde un iDRAC de una versión inferior a 2.3, primero es necesario actualizar el firmware del iDRAC a la versión 2.3 antes de actualizarlo a una versión 3.0 o superior.

El iDRAC (en un servidor) se reiniciará y no estará disponible temporalmente después de que se hayan cargado correctamente las actualizaciones de firmware.

Enlaces relacionados

Descarga de firmware del CMC

Visualización de versiones de firmware actualmente instaladas

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 → iKVM → Actualizar**

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

También es posible actualizar el firmware del iDRAC del servidor en **Descripción general del chasis → Descripción general del servidor → Actualizar**. Para obtener más información, consulte Actualización de firmware de los componentes del servidor.

2. Para actualizar el firmware del iDRAC6, en la sección **Firmware de iDRAC6 Enterprise**, active la casilla de la columna **Actualizar destinos** para el iKVM cuyo firmware desea actualizar, haga clic en **Aplicar actualización de iDRAC6 Enterprise** y desplácese al paso 4.
3. Para actualizar el firmware del iDRAC7, en la sección **Firmware de iDRAC7 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 de firmware de los componentes del servidor.
4. En el campo **Imagen del firmware**, introduzca la ruta de acceso del archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para dirigirse a la ubicación del archivo. El nombre predeterminado de la imagen del firmware del iDRAC es **firmimg.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 del iDRAC mediante RACADM, utilice el subcomando **fwupdate.** Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

Actualización de firmware de los componentes del servidor

Lifecycle Controller ofrece compatibilidad para actualización de módulos a través de iDRAC6 e iDRAC7. Se recomienda actualizar el firmware del CMC antes de actualizar los módulos de firmware de los componentes de los servidores. Después de actualizar el firmware del CMC, en la interfaz web del CMC, puede actualizar el firmware de los componentes de los servidores en la página **Descripción general del chasis → Descripción general de servidores → Actualizar → Actualizar componentes de servidores**. Además, se recomienda seleccionar de manera conjunta todos los módulos de los componentes de los servidores que se desean actualizar. Esto permitirá que Lifecycle Controller use algoritmos optimizados para actualizar el firmware, lo que reducirá la cantidad de reinicios.

NOTA: La versión del firmware del iDRAC6 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*.

NOTA: Para obtener información sobre cómo actualizar el firmware de componente del servidor, consulte, Flujo de trabajo recomendado para realizar actualizaciones en los servidores PowerEdge.

Enlaces relacionados

Activación de Lifecycle Controller
Filtrado de componentes para actualizaciones de firmware
Visualización del inventario de firmware
Operaciones de Lifecycle Controller
Actualización de firmware de los dispositivos de infraestructura de módulo de E/S

Activación 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 iDRAC6, cuando aparezca el mensaje `Pulsar <Ctrl+E> para Configuración de acceso remoto en 5 seg.`, pulse <Ctrl+E>. A continuación, en la pantalla de configuración, active **Servicios del sistema**.
- En la consola de inicio de los servidores iDRAC7, seleccione F2 para obtener acceso a Configuración del sistema. En la pantalla de configuración, seleccione **Configuración del iDRAC** y, a continuación, seleccione **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**.

En la página **Actualización de los componentes del servidor**, es posible actualizar varios componentes de firmware del sistema. Para utilizar las funciones y características de esta página, es necesario tener:

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

En caso de no tener privilegios suficientes, solo podrá ver el inventario de firmware de los componentes y los dispositivos en el servidor. No podrá seleccionar componentes ni dispositivos de ningún tipo de operación de Lifecycle Controller en el servidor.

Filtrado de componentes para actualizaciones de firmware

La información de todos los componentes y los dispositivos en todos los servidores se recupera de una sola vez. Para administrar esta gran cantidad de información, Lifecycle Controller proporciona varios mecanismos de filtrado. Estos filtros 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 filtro automático es importante al utilizar Dell Update Packages (DUP). La actualización de un paquete DUP se puede basar en el tipo o el modelo de un componente o dispositivo. El comportamiento de los filtros automáticos está diseñado para minimizar 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 para todos los servidores. Si el conjunto de servidores consiste en un número de modelos de servidores y se selecciona un servidor para la actualización del BIOS, la lógica del filtro automático quita los servidores que no coinciden con el modelo del servidor seleccionado. Esto garantiza que la selección de la imagen de actualización del firmware del BIOS (DUP) sea compatible con el modelo de servidor correcto.

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

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 **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

   La sección **Inventario de firmware** solo muestra los componentes o los dispositivos asociados en todos los servidores presentes en el chasis. El filtro es un filtro de pasada. Esto significa que solo permite los componentes o los dispositivos asociados con el filtro y excluye a todos los demás.

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

   Si no se selecciona ningún filtro y se selecciona un componente o dispositivo para su actualización en la sección de inventario, el filtro relacionado con esa selección se activa automáticamente. El filtrado puede continuar donde la sección de inventario muestra todos los servidores que coinciden con el componente seleccionado en modelo, tipo o alguna forma de identidad. Por ejemplo, si se selecciona un componente de BIOS en uno de los servidores para su actualización, el filtro se aplica en el BIOS automáticamente y la sección de inventario muestra los servidores que coinciden con el nombre de modelo del servidor seleccionado.

Filtrado de componentes para actualizaciones de firmware mediante RACADM

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

```
racadm getversion -l [-m <módulo>] [-f <filtro>]
```

Para obtener más información, consulte la RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) 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 **Inventario de firmware de componente/dispositivo**. En la tabla se muestran:

   - Los servidores que actualmente no admiten el servicio Lifecycle Controller se enumeran en **No admitido**. Se ofrece un hipervínculo a una página alternativa donde es posible actualizar de forma directa el firmware del iDRAC solamente. Esta página solo admite la actualización de firmware del iDRAC y de ningún otro componente o dispositivo en el servidor. La actualización de firmware del iDRAC no depende del servicio Lifecycle Controller.
   - Si el servidor se muestra como **No está listo**, esto indica que cuando se recuperó el inventario de firmware, el iDRAC del servidor aún se estaba inicializando. Espere hasta que iDRAC esté completamente operativo y actualice la página para recuperar el inventario de firmware nuevamente.
   - Si el inventario de componentes y dispositivos no refleja lo que está físicamente instalado en el servidor, es necesario invocar a Lifecycle Controller cuando el servidor está en proceso de inicio. Esto ayuda a actualizar la información de los componentes y los dispositivos internos, y permite verificar los componentes y los dispositivos instalados actualmente. Esta situación 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 iDRAC Configuration Utility (para iDRAC6) o iDRAC Settings Utility (para iDRAC7) proporcionan una opción a la que se puede obtener acceso mediante la consola de inicio:

     * En la consola de inicio de los servidores iDRAC6, cuando aparezca el mensaje `Pulsar <Ctrl +E> para Configuración de acceso remoto en 5 seg.`, pulse `<Ctrl+E>`. A continuación, en la pantalla de configuración, active **Recolectar inventario del sistema durante el reinicio**.
     * En la consola de inicio de los servidores iDRAC7, seleccione F2 para acceder a Configuración del sistema. En la pantalla de configuración, seleccione Configuración del iDRAC y, a continuación, seleccione Servicios del sistema (USC). En la pantalla de configuración, active **Recolectar inventario del sistema durante el reinicio**.
   - Se encuentran disponibles las opciones para las diversas operaciones de Lifecycle Controller como Actualizar, Revertir, Reinstalar y Eliminación de trabajos. Solamente se puede realizar un tipo de operación a la 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 9. : Información sobre componentes y dispositivos

Campo	Descripción
Ranura	Muestra la ranura que ocupa el servidor en el chasis. Los números de las ranuras son identificaciones consecutivas, de 1 a 16 (para las 16 ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis. Cuando 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 del dispositivo en el servidor. Si el ancho de la columna es demasiado estrecho, pase el mouse sobre la columna para ver la descripción completa.
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 cualquier operación que se ha programado en el servidor. El estado del trabajo se actualiza constantemente de forma dinámica. Si se detecta la compleción de un trabajo con el estado Completado, las versiones de firmware de los componentes y los dispositivos en ese servidor se actualizan automáticamente cuando se realiza un cambio de versión de firmware en alguno de los componentes o los dispositivos. También se expone un icono de información junto al estado actual, que proporciona información adicional sobre el estado del trabajo actual. Al hacer clic en el icono o mover el cursor sobre él, se puede ver esa 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 <módulo>] [-f <filtro>]
```

Para obtener más información, consulte la RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en **dell.com/support/manuals**.

Operaciones de Lifecycle Controller

Es posible realizar operaciones de Lifecycle Controller tales como:

- Reinstalar
- Revertir
- Actualizar
- Eliminar trabajos

Solamente se puede realizar un tipo de operación a la 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 vez que se ha programado una operación de Lifecycle Controller en un servidor, puede tardar de 10 a 15 minutos en completarse. El proceso implica varios reinicios del servidor mientras se instala el firmware, que también contiene una fase de verificación del firmware. Se puede observar el progreso del proceso en la consola del servidor. Si necesita actualizar varios componentes o dispositivos en un servidor, puede agrupar todas las actualizaciones en una operación programada y minimizar la cantidad de reinicios necesarios.

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

No se desplace a otra página después de enviar una operación para su programación. Si lo intenta, aparecerá un mensaje de confirmación en el que se puede cancelar la navegación. De lo contrario, se interrumpe la operación. Una interrupción, especialmente durante una operación de actualización, puede finalizar la carga del archivo de imagen del firmware antes de tiempo. Después de enviar una operación para su programación, asegúrese de aceptar el mensaje de confirmación emergente para indicar que la operación se ha programado correctamente.

Enlaces relacionados

Reinstalación del firmware de los componentes del servidor
Reversión del firmware de los componentes del servidor
Actualización de firmware de los componentes del servidor
Eliminación de trabajos programados sobre el firmware de los componentes del servidor

Reinstalación del firmware de los componentes del servidor

Es posible volver a instalar la imagen de firmware del firmware actualmente instalado para componentes o dispositivos seleccionados en uno o varios servidores. La imagen de firmware está disponible dentro de Lifecycle Controller.

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

Para volver a instalar el firmware de los componentes 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 marcación del componente o dispositivo para el cual desea volver a instalar el firmware.
4. Seleccione una de las opciones siguientes:
   - **Reiniciar ahora**: se realiza un reinicio de inmediato.
   - **En el próximo reinicio**: se reinicia manualmente el servidor en otro momento.
5. Haga clic en **Reinstalar**. La versión del firmware se vuelve a instalar para el componente o dispositivo seleccionado.

Reversión del firmware de los componentes del servidor

Es posible instalar la imagen de firmware del firmware previamente instalado para componentes o dispositivos seleccionados en uno o varios servidores. La imagen de firmware está disponible en 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**.

   Aparecerá la página **Actualización de los componentes del servidor**.
2. Filtre el componente o el dispositivo (opcional).
3. En la columna **Revertir versión**, active la casilla del componente o dispositivo para el cual desea revertir el firmware.
4. Seleccione una de las opciones siguientes:

   - **Reiniciar ahora**: se realiza un reinicio de inmediato.
   - **En el próximo reinicio**: se reinicia manualmente el servidor en otro momento.
5. Haga clic en **Revertir**. La versión del firmware previamente instalada se vuelve a instalar para el componente o dispositivo seleccionado.

Actualización de firmware de los componentes del servidor

Es posible instalar la siguiente versión de la imagen de firmware para los componentes o los dispositivos seleccionados en 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.

Se recomienda borrar la cola de trabajos antes de iniciar una actualización de firmware de los componentes en el servidor. En la página Trabajos de Lifecycle Controller, se ofrece una lista de todos los trabajos en el servidor. Esta página permite borrar uno o varios trabajos, o purgar todos los trabajos en el servidor. Consulte la sección de Solución de problemas, "Managing Lifecycle Controller jobs on a remote system" (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 a la vez en un servidor, el tamaño combinado de todos los archivos de actualización de firmware puede superar los 48 MB. En ese caso, una de las actualizaciones en el componente falla, ya que el archivo de actualización se trunca. Una estrategia recomendada para actualizar varios componentes en un servidor es primero actualizar juntos los componentes de Diagnósticos de 32 bits y Lifecycle Controller. Estas actualizaciones no requieren reiniciar el servidor y se completan relativamente rápido. Los demás componentes pueden actualizarse juntos después.

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

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

Para actualizar la versión de firmware a la siguiente versión:

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. Filtre el componente o el dispositivo (opcional).
3. En la columna **Actualizar**, seleccione las casillas para el componente o el dispositivo en el que desea actualizar el firmware a la siguiente versión. Utilice el acceso directo con la tecla CRTL para seleccionar un tipo de componente o dispositivo que se actualice en todos los servidores aplicables. Si mantiene presionada la tecla CRTL, se resaltan todos los componentes en amarillo. Mientras mantiene presionada la tecla CRTL, active la casilla asociada en la columna **Actualizar** para seleccionar el componente o el dispositivo necesario.

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

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

   NOTA: El límite de tamaño de la actualización para un solo DUP o varios DUP combinados se puede ignorar si la función Almacenamiento extendido está instalada y activada. Para obtener información sobre la forma de activar el almacenamiento extendido, consulte Configuring CMC Extended Storage Card (Configuración de la tarjeta de almacenamiento extendido del CMC).
4. Especifique el archivo de imagen de firmware para los componentes o los dispositivos seleccionados. Este es un archivo de Dell Update Packages (DUP) para Microsoft Windows.
5. Seleccione una de las opciones siguientes:
   - **Reiniciar ahora**: se realiza un reinicio de inmediato.
   - **En el próximo reinicio**: se reinicia manualmente el servidor en otro momento.

   NOTA: Este paso no es válido para las actualizaciones de firmware en Diagnósticos de 32 bits y Lifecycle Controller. Para estos componentes, se reinicia inmediatamente el servidor.
6. Haga clic en **Actualizar**. Se actualizará la versión de firmware para el componente o el 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. Filtre el componente o el dispositivo (opcional).
3. En la columna **Estado de trabajo**, si se muestra una casilla junto al estado del trabajo, significa que existe un trabajo de Lifecycle Controller en progreso y se encuentra en el estado indicado. Se puede seleccionar para una operación de eliminación de trabajos.
4. Haga clic en **Eliminación de trabajos**. Se eliminarán los trabajos para los componentes o los dispositivos seleccionados.

Recuperación de firmware del iDRAC mediante el CMC

El firmware del iDRAC se actualiza normalmente a través de las capacidades del iDRAC, como la interfaz web del iDRAC, la interfaz de línea de comandos SM-CLP o los paquetes de actualización específicos del sistema operativo

descargados de **support.dell.com**. Para obtener más información, consulte iDRAC User's Guide (Guía del usuario del iDRAC).

Las generaciones tempranas de servidores pueden recuperar el firmware dañado mediante el nuevo proceso de actualización de firmware del iDRAC. Cuando el CMC detecta el firmware dañado del iDRAC, indica el servidor en la página **Actualización del firmware**. Realice los pasos mencionados 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

Visualización de los resúmenes de los componentes del chasis

Al iniciar sesión en la interfaz web del CMC, la página **Condición del chasis** permite ver la condición del chasis y de sus componentes, Además, muestra una vista gráfica en directo del chasis y de sus componentes. Esta vista se actualiza de forma dinámica. El subgráfico de los componentes se superpone y se modifican automáticamente las sugerencias de texto para reflejar el estado actual.

Ilustración 1. Ejemplo de gráficos de chasis en la interfaz web

Para ver la condición del chasis, vaya a **Descripción general del chasis** → **Propiedades** → **Condición**. Se mostrará el estado de condición general del chasis, los CMC activos 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 del CMC. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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

Gráficos del chasis

Las vistas frontal y posterior (las imágenes superior e inferior, respectivamente) representan el chasis. Los servidores y la pantalla LCD se muestran en la vista frontal y los demás componentes se muestran en la vista posterior. La selección de cada componente se indica con el color azul y se controla al hacer clic sobre la imagen del componente requerido. 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) en la que está instalado. Las posiciones vacías se indican con un fondo de color gris oscuro. 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 apoyar el cursor sobre un componente aparecerá información adicional sobre ese componente.

Tabla 10. : Estados del icono del servidor

Icono	Descripción
	El servidor está encendido y funciona normalmente.
	El servidor está apagado.
	El servidor indica un error no crítico.
	El servidor indica un error crítico.

Icono	Descripción
	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.
- Vínculos rápidos: proporciona vínculos para navegar hasta las páginas con mayor acceso y hasta las acciones realizadas con mayor frecuencia. Esta sección solo muestra los vínculos aplicables al componente seleccionado.

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) se mostrarán en la lista expandida Servidores. El nombre de una ranura sin servidor se mostrará en gris.
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 **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 **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**.
   La página **Condición del chasis** mostrará una descripción gráfica de todos los servidores instalados en el chasis. El estado de condición de los servidores se indica con la superposición del subgráfico de los servidores. 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 **Estado de los servidores** proporciona descripciones generales de los servidores en 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 servidor individual

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

1. Vaya a **Descripción general del chasis** → **Propiedades** → **Condición**.
   La página **Condición del chasis** mostrará una descripción gráfica de todos los servidores instalados en el chasis. El estado de condición de cada servidor se indica con la superposición del subgráfico del servidor. Mueva el cursor sobre el subgráfico de un servidor individual. La sugerencia de texto o la explicación en pantalla correspondiente brinda información adicional sobre ese servidor. Haga clic en el subgráfico del servidor para ver la información del módulo de E/S a la derecha. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
2. Vaya a **Descripción general del chasis** y expanda **Descripción general del servidor** en el árbol del sistema. Todos los servidores (de 1 a 16) aparecerán en la lista expandida. Haga clic en el servidor (la ranura) que desea ver.
   La página **Estado del servidor** (separada de la página **Estado de los servidores**) proporciona el estado de condición del servidor en el chasis y un punto de inicio para la interfaz web del iDRAC, que 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, es necesario disponer de un nombre de usuario y una contraseña del iDRAC. Para obtener más información sobre el iDRAC y la forma de usar la interfaz web del iDRAC, 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**.
   La página **Condición del chasis** mostrará una descripción gráfica de todos los servidores instalados en el chasis. El estado de condición de cada servidor se indica con la superposición del subgráfico del servidor. Mueva el cursor sobre el subgráfico de un servidor individual. La sugerencia de texto o la explicación en pantalla correspondiente brinda información adicional sobre ese servidor. Haga clic en el subgráfico del servidor para ver la información del

módulo de E/S a la derecha. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

2. Vaya a **Descripción general del chasis** y expanda **Descripción general del servidor** en el árbol del sistema. Todas las ranuras (de 1 a 16) aparecerán en la lista expandida. Haga clic en la ranura donde se encuentra insertado el arreglo de almacenamiento.

   La página Estado de arreglo de almacenamiento muestra el estado de 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 del CMC, realice alguno de los siguientes pasos:

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

   Aparecerá la página **Condición del chasis**. En la sección inferior de **Gráficos del chasis**, se ilustra la vista posterior del chasis y se incluye el estado de condición de los módulos de E/S. El estado de condición de un módulo de E/S se indica con la superposición del subgráfico del módulo de E/S. Mueva el cursor sobre el subgráfico de un módulo de E/S individual. El texto de la sugerencia ofrece información adicional sobre ese módulo de E/S. Haga clic en el subgráfico del módulo de E/S para ver la información del módulo de E/S a la derecha.

2. Vaya a **Descripción general del chasis** → **Descripción general del módulo de E/S** → **Propiedades** → **Estado**.

   La página **Estado del módulo 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 **Condición del chasis**. En la sección inferior de Gráficos del chasis, se ilustra la vista posterior del chasis y se incluye el estado de condición de los módulos de E/S. El estado de condición de un módulo de E/S se indica con la superposición del subgráfico del módulo de E/S. Mueva el cursor sobre el subgráfico de un módulo de E/S individual. El texto de la sugerencia ofrece información adicional sobre ese módulo de E/S. Haga clic en el subgráfico del módulo de E/S para ver la información del módulo de E/S a la derecha.

2. Vaya a **Descripción general del chasis** y expanda **Descripción general del módulo de E/S** en el árbol del sistema. Todos los módulos de E/S (de 1 a 6) aparecerán en la lista expandida. Haga clic en el módulo de E/S (la ranura) que desea ver.

   Aparecerá la página **Estado del módulo de E/S** (separada de la página general **Estado del módulo de E/S**) específica de la ranura del módulo de E/S. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualización de información y estado de condición de los ventiladores

El CMC, que controla la velocidad de los ventiladores, aumenta o disminuye automáticamente la velocidad de estos en función de los sucesos que se producen en todo el sistema. El CMC genera una alerta y aumenta la velocidad de los ventiladores cuando se producen los siguientes sucesos:

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

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

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

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

   Aparecerá la página **Condición del chasis**. En la sección inferior de Gráficos del chasis, se muestra una vista posterior del chasis y se incluye el estado de condición del ventilador. El estado de condición del ventilador se indica con la superposición del subgráfico del ventilador. Mueva el cursor sobre el subgráfico del ventilador. La sugerencia de texto ofrece información adicional sobre el ventilador. Haga clic en el subgráfico del ventilador para ver la información del ventilador a la derecha.
2. Vaya a **Descripción general del chasis** → **Ventiladores** → **Propiedades**.

   La página **Estado de los ventiladores** proporciona el estado y las mediciones de velocidad (en revoluciones por minuto o RPM) de los ventiladores en el 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 **Condición del chasis**. En la sección inferior de los gráficos del chasis, se muestra una vista posterior del chasis y se incluye el estado de condición del iKVM. El estado de condición del iKVM se indica con la superposición del subgráfico del iKVM. Mueva el cursor sobre el subgráfico de un iKVM. Se mostrará la sugerencia de texto o la explicación en pantalla correspondiente. La sugerencia de texto ofrece información adicional sobre el iKVM. Haga clic en el subgráfico del iKVM para ver la información del iKVM a la derecha.
2. Vaya a **Descripción general del chasis** → **iKVM** → **Propiedades**.

   La página **Estado del iKVM** mostrará 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 **Condición del chasis**. En la sección inferior de los gráficos del chasis, se muestra una vista posterior del chasis y se incluye el estado de condición de todas las PSU. El estado de condición de cada PSU se indica con la superposición del subgráfico de la PSU. Mueva el cursor sobre el subgráfico de una PSU individual. Se mostrará la sugerencia de texto o la explicación en pantalla correspondiente. La sugerencia de texto ofrece información adicional sobre esa PSU. Haga clic en el subgráfico de la PSU para ver la información de la PSU a la derecha.
2. Vaya a **Descripción general del chasis** → **Suministros de energía**.
   La página **Estado de suministros de energía** mostrará el estado y las lecturas de las PSU asociadas con el chasis. Se proporcionará 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 **Estado de sensores de temperatura** mostrará el estado y las lecturas 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 puede generar una alerta que puede causar que la velocidad de los ventiladores varíe. Por ejemplo, cuando la sonda de temperatura ambiente del CMC supera el umbral, la velocidad de los ventiladores del 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 **Condición del chasis**. En la sección superior de Gráficos del chasis, se ilustra la vista frontal del chasis. El estado de condición de la pantalla LCD se indica con la superposición del subgráfico de la pantalla LCD.
2. Mueva el cursor sobre el subgráfico de la pantalla LCD. La sugerencia de texto o la explicación en pantalla correspondiente brinda información adicional sobre la pantalla LCD.
3. Haga clic en el subgráfico de la pantalla LCD para ver la información de la pantalla LCD 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 el CMC, es necesario definir los valores de configuración de red del CMC para que el CMC pueda administrarse de manera remota. La configuración inicial asigna los parámetros de red TCP/IP que permiten el acceso al CMC. Para obtener más información, consulte Setting Up Initial Access to CMC (Configuración del acceso inicial al CMC).

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

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

Enlaces relacionados

Inicio de sesión en el CMC
Visualización y modificación de la configuración de red LAN del CMC
Configuración de las opciones de red y de seguridad de inicio de sesión del CMC
Configuración de las propiedades de la etiqueta LAN virtual para CMC
Configuración de servicios
Configuración de los LED para identificar componentes en el chasis
Configuración de un grupo de chasis
Configuración del servidor
Administración de la red Fabric de E/S
Configuración y uso de iKVM
Obtención de certificados
Configuración de cuentas de usuario y privilegios
Configuración del CMC para enviar alertas
Administración y supervisión de la alimentación
Configuración de varios CMC mediante RACADM

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 al 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 del 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 del 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 del CMC mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del chasis?** y haga clic en **Red** → **Red**. La página **Configuración de la red** mostrará la configuración de red actual.
2. Modifique la configuración general de IPv4 o IPv6, según sea necesario. 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 y modificación de la configuración de red LAN del CMC mediante RACADM

Para ver la configuración de IPv4, use los siguientes subcomandos y objetos:

- `getniccfg`
- `getconfig`
- cfgCurrentLanNetworking

Para ver la configuración de IPv6, use los siguientes subcomandos y objetos:

- `getconfig`
- cfgIPv6LanNetworking

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

Para obtener más información sobre los subcomandos y objetos, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

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: El NIC del 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 del CMC está desactivado de forma predeterminada.

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

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

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g
cfgLanNetworking -o cfgNicIpAddress <dirección IP estática> racadm config -g
cfgLanNetworking -o cfgNicGateway <puerta de enlace estática> racadm config -g
cfgLanNetworking -o cfgNicNetmask <máscara de subred estática>
```

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 el CMC, escriba:

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

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

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

Se puede desactivar la función DHCP para la dirección de NIC y especificar dirección IP, máscara de subred y puerta de enlace estáticas. Para obtener más información, consulte Setting Up Initial Access to CMC (Configuración del acceso inicial al CMC).

Activación o desactivación de DHCP para las direcciones IP de DNS

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

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

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

Para 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 <dirección-IP> racadm config
-g cfgLanNetworking -o cfgDNSServer2 <dirección-IPv4>
```

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

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

Configuración de DNS (IPv4 e IPv6)

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

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

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

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

- **Nombre del CMC**: de forma predeterminada, el nombre del CMC en el servidor DNS es cmc-<*etiqueta de servicio*>. Para cambiar el nombre del CMC en el servidor DNS, escriba:

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

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

- **Nombre de dominio DNS**: el nombre de dominio DNS predeterminado es un carácter en blanco único. Para establecer un nombre de dominio DNS, escriba:

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

  donde <nombre> 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 (IPv4 e IPv6)

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

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

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0 racadm config -g
cfgNetTuning -o cfgNetTuningNicFullDuplex <modo dúplex>
```

donde:

<modo dúplex> es 0 (dúplex medio) o 1 (dúplex completo, valor predeterminado)

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

donde:

<velocidad> es 10 o 100 (valor predeterminado).

Configuración de la unidad de transmisión máxima (MTU) (IPv4 e IPv6)

La propiedad MTU permite establecer un límite para el paquete más grande que se puede transferir a través de 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, el 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 el CMC le permiten evitar problemas de seguridad provocados por intentos de ataques de contraseñas. Esta función le permite bloquear un rango de direcciones IP y de usuarios que pueden acceder al CMC. De manera predeterminada, la función de bloqueo de direcciones IP está activada en el CMC.

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

Puede configurar los atributos del rango de IP con la interfaz web del CMC o con RACADM. Para usar las funciones de bloqueo de direcciones IP y de bloqueo de usuarios, active las opciones con la interfaz web del CMC o con RACADM. Configure las opciones de la política de bloqueo de inicio de sesión para establecer la cantidad de intentos de inicio de sesión incorrectos para un usuario o una dirección IP específicos. Superado este límite, el usuario bloqueado podrá iniciar sesión solo después de expirado el tiempo de penalidad.

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 **Descripción general del chasis** y haga clic en **Red** → **Red**. Aparecerá la página **Configuración de la red**.
2. En la sección Configuración de IPv4, haga clic en **Opciones avanzadas**.
   Aparecerá la página **Seguridad de inicio de sesión**.
   De manera alternativa, para acceder a la página Seguridad de inicio de sesión, en el árbol del sistema, diríjase a **Descripción general del chasis** y haga clic en **Seguridad** → **Inicio de sesión**.
3. Para activar la función de verificación de rango de IP, en la sección **Rango de IP**, seleccione la opción **Rango de IP activado**.
   Se activarán los campos **Dirección de rango de IP** y **Máscara de rango de IP**.
4. En los campos **Dirección de rango de IP** y **Máscara de rango de IP**, escriba el rango de direcciones IP y de máscaras de rangos de IP para los que desea bloquear el acceso al CMC.
   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el 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. Un inicio de sesión desde la dirección IP entrante se permite solo si los siguientes valores son idénticos:

- **cfgRacTuneIpRangeMask** en cantidad de bits y con la dirección IP entrante
- **cfgRacTuneIpRangeMask** en cantidad de bits y con **cfgRacTuneIpRangeAddr**

NOTA:

- Para activar la función de verificación de rango IP, use la siguiente propiedad en el grupo `cfgRacTuning`:
  `cfgRacTuneIpRangeEnable <0/1>`
- Para especificar el rango de direcciones IP para las que desea bloquear el acceso al CMC, use la siguiente propiedad en el grupo `cfgRacTuning`:
  `cfgRacTuneIpRangeAddr`
- Para especificar la máscara del rango de IP para el que desea bloquear el acceso al 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, vaya a **Descripción general del chasis?** y haga clic en **Red** → **VLAN**?.
   - En el árbol del sistema, vaya a **Descripción general del chasis** → **Descripción general del servidor** y haga clic en **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 red VLAN para el CMC, establezca la prioridad y asigne la identificación. Para obtener más información sobre los campos, consulte *CMC Online Help (Ayuda en línea para el 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 <Id de VLAN>
   ```
   Los valores válidos para <Id de VLAN> son 1 a 4000 y 4021 a 4094. El valor predeterminado es 1.
   Por ejemplo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID 1
   ```
3. A continuación, especifique la prioridad de VLAN para la red de administración del chasis externo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority <Prioridad de VLAN>
   ```
   Los valores válidos para <Prioridad de VLAN> son de 0 a 7. El valor predeterminado es 0.
   Por ejemplo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7
   ```
   También puede especificar la identificación y la prioridad de VLAN con un solo comando:
   ```
   racadm setniccfg -v <Id de VLAN> <Prioridad de VLAN>
   ```
   Por ejemplo:
   ```
   racadm setniccfg -v 1 7
   ```
4. Para eliminar la VLAN del CMC, desactive las capacidades de VLAN de la red de administración del chasis externo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 0
   ```
   También puede eliminar la VLAN del CMC con el siguiente comando:
   ```
   racadm setniccfg -v
   ```

Configuración de servicios

Es posible configurar y activar los servicios siguientes en el CMC:

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

El CMC incluye un componente Web Server que está configurado para utilizar el protocolo de seguridad SSL estándar en el sector para aceptar y transferir datos cifrados desde y hacia los clientes por Internet. Web Server incluye un certificado digital SSL autofirmado de Dell™ (identificación de servidor) y es responsable de aceptar y responder las solicitudes de HTTP seguro de los clientes. La interfaz web y la herramienta CLI remota de RACADM requieren este servicio para comunicarse con el CMC.

Si se restablece Web Server, espere al menos un minuto para que los servicios vuelvan a estar disponibles. En general, Web Server se restablece como resultado 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 restableció el CMC.
- Se cargó 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 el CMC. Después de configurar el syslog remoto, cada nueva anotación de registro generada por CMC se reenviará 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, vaya a **Descripción general del chasis** y haga clic en **Red** → **Servicios**. Aparecerá la página **Servicios**.
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 sobre estos objetos, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)* disponible en **dell.com/support/manuals**.

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

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

Por ejemplo:

```
$ racadm getconfig -g cfgSessionManagement -m server-1 #
cfgSsnMgtWebServerMaxSessions=N/A # cfgSsnMgtWebServerActiveSessions=N/A #
```

```
cfgSsnMgtWebServerTimeout=N/A # cfgSsnMgtSSHMaxSessions=N/A #
cfgSsnMgtSSHActiveSessions=N/A # cfgSsnMgtSSHTimeout=N/A #
cfgSsnMgtTelnetMaxSessions=N/A # cfgSsnMgtTelnetActiveSessions=N/A #
cfgSsnMgtTelnetTimeout=N/A
```

Configuración de la tarjeta de almacenamiento extendido del CMC

Es posible activar o reparar los medios flash extraíbles opcionales para utilizarlos como un almacenamiento extendido no volátil. Algunas funciones del CMC dependen de un almacenamiento extendido no volátil para funcionar.

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

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Controladora del chasis** → **Medios flash**. Aparecerá la página 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 presentes en el chasis, ambos deben contener un medio flash. Las funciones del CMC que dependen de los medios flash (excepto Flexaddress), no funcionan correctamente hasta que se instala y se activa en esta página un medio autorizado por Dell.

Configuración de un grupo de chasis

El CMC permite controlar varios chasis desde un solo chasis principal. Cuando se activa un grupo de chasis, el 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 el signo ! 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 **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 contener hasta ocho miembros. Además, un chasis principal o miembro solo puede participar en un grupo. No se puede unir un chasis, ya sea principal o miembro, a otro grupo si ya forma parte de otro grupo. Es posible eliminar el chasis de un grupo y agregarlo más adelante a un grupo diferente.

Para configurar el grupo de chasis mediante la interfaz web 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 **Grupo de chasis**.
3. En la página **Grupo de chasis**, en **Función**, seleccione **Principal**. Aparecerá un campo para agregar el nombre de grupo.

4. Introduzca el nombre de grupo en el campo **Nombre del grupo** y haga clic en **Aplicar**.

   NOTA: Los nombres de dominio siguen las mismas reglas.

   Cuando se crea un grupo de chasis, la interfaz gráfica de usuario cambia automáticamente a la página **Grupo de chasis**. El árbol del sistema indica el grupo por nombre de grupo, y el chasis principal y el chasis miembro desocupado aparecerán en el árbol del sistema.

Enlaces relacionados

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

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**.
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 los pasos 4 a 8 para agregar un máximo de ocho miembros. Los nombres de chasis de los miembros nuevos aparecerán en el cuadro de diálogo **Miembros**.

   Al seleccionar un grupo del 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 deben aprobar de forma segura en el chasis miembro, para establecer una relación de confianza entre el miembro y el chasis principal. Las credenciales no se conservan en ninguno de los chasis y no se vuelven a intercambiar una vez que se establece la relación de confianza.

   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

Es posible eliminar un miembro del grupo desde el chasis principal. Para eliminar un miembro:

1. Inicie sesión en el chasis principal con los privilegios de administrador de chasis.
2. 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 establecerá una conexión con el miembro o los miembros, si se selecciona más de uno, que se hayan eliminado del grupo. El nombre del miembro desaparece. Si no se produce un contacto entre el miembro y el chasis principal debido a un problema en la red, es posible que el chasis miembro no reciba el mensaje. Si esto sucede, desactive el miembro del chasis miembro para poder eliminarlo totalmente.

Enlaces relacionados

Desactivación de un miembro del chasis miembro

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 se comunicará con todos los miembros que se hayan quitado del grupo. Finalmente, el chasis principal finalizará su función. Ahora es posible nombrarlo como miembro o líder de otro grupo.

   Si un problema en la red evita que se produzca un contacto entre el miembro y el líder, es posible que el chasis miembro no reciba el mensaje. En ese caso, desactive el miembro del chasis miembro para poder quitarlo totalmente.

Desactivación de un miembro del chasis miembro

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

1. Inicie sesión en el chasis miembro con privilegios de administrador.
2. 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 a la página web de un chasis miembro, la consola remota de un servidor o la pagina web de un iDRAC del servidor dentro del grupo se encuentran disponibles en la página del grupo del chasis principal. Es posible utilizar el nombre de usuario y la contraseña con los que se inició sesión en el chasis principal para iniciar sesión en el dispositivo miembro. Si el dispositivo miembro tiene las mismas credenciales de inicio de sesión, no es necesario un inicio adicional. De lo contrario, el usuario es dirigido 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 un CMC miembro, seleccione **Iniciar CMC** para el chasis necesario.

   Si el destino necesario es un servidor en un chasis, realice lo siguiente:

   a) Seleccione la imagen del chasis de destino.
   b) Seleccione el servidor en la imagen del chasis que aparece debajo del panel **Condición y alertas**.
   c) En el cuadro con la etiqueta **Vínculos rápidos**, seleccione el dispositivo de destino. Aparecerá una nueva ventana con la pantalla de inicio de sesión o la página de destino.

Propagación de las propiedades del chasis principal al chasis miembro

Puede aplicar las propiedades del chasis principal al chasis miembro de un grupo. Para sincronizar un miembro con las propiedades del chasis principal:

1. Inicie sesión en el chasis principal con privilegios de administrador.
2. Seleccione el chasis principal en el árbol.
3. Haga clic en **Configuración → Administración de grupos**.
4. En la sección **Propagación de las propiedades del chasis** seleccione un tipo de propagación:
   - Propagación ante cambio: seleccione esta opción para propagar automáticamente la configuración de las propiedades del chasis seleccionadas. Los cambios de propiedades se propagan a todos los miembros del grupo actual cada vez que cambien las propiedades del chasis principal.
   - Propagación manual: seleccione esta opción para propagar manualmente las propiedades del chasis principal del grupo con sus miembros. La configuración de las propiedades del chasis principal se propagan a los miembros del grupo solo cuando el administrador del chasis principal hace clic en **Propagar**.
5. En la sección **Propiedades de propagación**, seleccione las categorías de las propiedades de configuración del chasis principal a propagar a los chasis miembro.

   Seleccione solo las categorías de configuración que configuró de manera idéntica en todos los miembros del grupo de chasis. Por ejemplo, seleccione la categoría **Propiedades de registro y alerta**, para permitir que todos los chasis del grupo compartan la configuración de registro y alerta del chasis principal.
6. Haga clic en **Guardar**.

   Si está seleccionada la opción **Propagación ante cambio**, el chasis miembro toma las propiedades del chasis principal. Si está seleccionada la opción **Propagación manual**, haga clic en **Propagar** cada vez que desee propagar la configuración elegida al chasis miembro. Para obtener más información sobre la Propagación de propiedades del chasis líder a los chasis miembro, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Inventario del servidor para el grupo de administración de múltiples chasis

En la página Condición del grupo de chasis se muestran todos los chasis miembro y se puede guardar el informe de inventario del servidor en un archivo, con la capacidad de descarga estándar del explorador. El informe contiene datos para:

- Todos los servidores presentes actualmente en todos los chasis del grupo (incluido el principal).
- 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:

Tabla 11. : Descripciones de campos en el inventario de blade

Campo de datos	Ejemplo
Nombre del chasis	Chasis principal del centro de datos
Dirección IP del chasis	192.168.0.1
Ubicación de ranura	1
Nombre de ranura	RANURA-01
Nombre del host	Web Server corporativo **NOTA:** Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.
Sistema operativo	Windows Server 2008 **NOTA:** Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.
Modelo	PowerEdgeM610
Etiqueta de servicio	1PB8VF1
Memoria total del sistema	4.0 GB **NOTA:** Requiere CMC 4.0 (o superior) en el miembro; de lo contrario, se mostrará en blanco.
N.º de CPU	2

Campo de datos	Ejemplo
	NOTA: Requiere CMC 4.0 (o superior) en el miembro; de lo contrario, se mostrará en blanco.
Información de CPU	CPU Intel (R) Xeon (R) E5502 a 1.87 GHzn
	NOTA: Requiere CMC 4.0 (o superior) en el miembro; de lo contrario, se mostrará en blanco.

Formato de datos

El informe de inventario se genera en un formato de archivo **.CSV**, de modo que se pueda importar en varias herramientas, por ejemplo, Microsoft Excel. El archivo **.CSV** del informe de inventario se puede importar en la plantilla al seleccionar **Datos** → **Desde texto** en MS Excel. Una vez que el informe de inventario se haya importado en MS Excel y aparezca un mensaje para solicitar información adicional, seleccione Delimitado por comas para importar el archivo en MS Excel.

Inventario del grupo de chasis y versión de firmware

La página **Versión de firmware de grupo de chasis** muestra el inventario de grupos y las versiones de firmware de los servidores, además de los componentes del servidor en el chasis. Esta página también le permite organizar la información de inventario y filtrar la vista de las versiones de firmware. La vista mostrada puede basarse en los servidores o en cualquiera de los siguientes componentes del servidor del chasis:

- BIOS
- iDRAC
- CPLD
- USC
- Diagnostics (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 con la interfaz web de CMC, en el árbol del sistema, seleccione **Grupo**. Haga clic en **Propiedades** → **Versión de firmware**. Aparecerá la página **Versión de firmware del grupo de chasis**, que 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 **Grupo**. Haga clic en **Propiedades** → **Versión de firmware**.
   La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.
2. En la sección **Seleccionar un chasis**, seleccione el chasis miembro del que desea ver el inventario.

La sección **Filtro de visualización de firmware** muestra el inventario de servidor del chasis seleccionado y las versiones de firmware de todos los componentes del servidor.

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

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

1. En el árbol del sistema, seleccione **Grupo**. Haga clic en **Propiedades → Versión de firmware**.
   La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.
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 10ma 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 del CMC de un chasis miembro es anterior a la versión 4.45. En este caso, no aparecerán los componentes de ninguno de los servidores en este chasis, incluso si los servidores admiten Lifecycle Controller.

Obtención de certificados

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

Tabla 12. : Tipos de inicio de sesión y de 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.

Tipo de inicio de sesión	Tipo de certificado	Cómo obtenerlo
Inicio de sesión de usuario local	Certificado SSL	Generar una CSR y hacer que la firme una CA de confianza **NOTA:** Junto con el CMC, se envía un certificado de servidor SSL autofirmado predeterminado. Web Server y la consola virtual del CMC utilizan este certificado.

Enlaces relacionados

Certificados de servidor de capa de sockets seguros (SSL)

Certificados de servidor de capa de sockets seguros (SSL)

El CMC incluye un componente Web Server que está configurado para utilizar el protocolo de seguridad SSL estándar en el sector para transferir datos cifrados a través de Internet. SSL se basa en la tecnología de cifrado de claves públicas y privadas y es una técnica ampliamente aceptada para ofrecer comunicación cifrada y autentificada entre los clientes y los servidores a fin de evitar escuchas ilegales en una red.

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 de datos. El CMC emplea el estándar de cifrado SSL de 128 bits, la forma de cifrado más segura generalmente disponible para los exploradores web en Norteamérica.

El componente Web Server del CMC incluye un certificado digital SSL autofirmado de Dell (identificación de servidor). Para garantizar alta seguridad en Internet, sustituya el certificado SSL de Web Server mediante el envío de una solicitud al 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 mostrará el nombre común como <nombre_del_cmc.nombre_del_dominio>, donde nombre_del_cmc es el nombre del host de CMC y nombre_del_dominio es el nombre del dominio. Si el nombre del dominio no está disponible, se mostrará solamente el nombres de dominio parcial (PQDN), que es el nombre del host del CMC.

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una autoridad de certificados (denominada CA en la interfaz web) para obtener un certificado de servidor seguro. Los certificados de servidor seguro garantizan la identidad de un sistema remoto y garantizan que otros usuarios no puedan ver o cambiar la información intercambiada con dicho sistema. Para garantizar la seguridad del CMC, se recomienda enfáticamente generar una CSR, enviarla a una autoridad de certificados y cargar el certificado que se reciba de la autoridad de certificados.

Una autoridad de certificados es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis fiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de

autoridades de certificados se incluyen Thawte y VeriSign. Una vez que la autoridad de certificados recibe la solicitud de firma de certificado, la revisa y verifica la información contenida en la solicitud. Si el solicitante cumple con los estándares de seguridad de la autoridad de certificados, la autoridad emite un certificado que identifica al solicitante de manera exclusiva para realizar transacciones a través de redes y en Internet.

Después de que la autoridad de certificados aprueba la solicitud de firma de certificado y le envía un certificado, usted debe cargar el certificado en el firmware del CMC. La información de la solicitud de firma de certificado almacenada en el firmware del CMC debe coincidir con la información contenida 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.

Enlaces relacionados

Generación de una nueva solicitud de firma de certificado
Carga del certificado del servidor
Visualización del certificado del servidor

Generación de una nueva solicitud de firma de certificado

Para garantizar la seguridad, se recomienda obtener y cargar un certificado de servidor seguro en el CMC. Los certificados de servidor seguros garantizan la identidad de un sistema remoto y que terceros no puedan ver ni cambiar la información que se intercambia con el sistema remoto. Sin un certificado de servidor seguro, el CMC es vulnerable al acceso de usuarios no autorizados.

Para obtener un certificado de servidor seguro para el CMC, es necesario enviar una solicitud de firma de certificado (CSR) a la autoridad de certificados que se elija. Una CSR es una solicitud digital de un certificado de servidor seguro firmado que contenga información sobre la organización y una clave de identificación exclusiva.

Una vez generada la CSR, se le pedirá al usuario que guarde una copia de la CSR en la estación de administración o en la red compartida y la información exclusiva que se utilizó para generar la CSR se almacenará en el CMC. Esta información se utilizará posteriormente para autentificar el certificado de servidor que se recibe de la autoridad de certificados. Después de recibir el certificado de servidor de la autoridad de certificados, es necesario cargarlo en el 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, esta sobrescribe la CSR anterior en el CMC. Si una CSR pendiente se sobrescribe antes de que la autoridad de certificados otorgue su certificado de servidor, el CMC no aceptará el certificado de servidor porque la información que usa para autentificar el certificado se ha perdido. Tome precauciones al generar una 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, vaya a **Descripción general del chasis** y haga clic en **Red → SSL**. Aparecerá **Menú principal de SSL**.
2. Seleccione **Generar una nueva solicitud de firma de certificado (CSR)** y haga clic en **Siguiente**. Aparecerá la página **Generar una solicitud de firma de certificado (CSR)**.
3. Escriba un valor para cada atributo de la CSR.
4. Haga clic en **Generar**. Aparecerá un cuadro de diálogo **Descarga de archivo**.
5. Guarde el archivo **csr.txt** en la estación de administración o en la red compartida. (También puede abrir el archivo en este momento 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 *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)* disponible en **dell.com/support/manuals**.

Carga del certificado del servidor

Después de generar una CSR, puede cargar el certificado del servidor SSL firmado al firmware del CMC. El CMC se restablece una vez que se carga el certificado. El CMC solo acepta certificados de servidor web codificado con X509, Base 64.

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

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, vaya a **Descripción general del chasis** y haga clic en **Red → SSL**. Aparecerá **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 **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo de certificado que se desea cargar. Debe escribir la ruta de acceso absoluta del archivo, lo que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

Carga del certificado del servidor mediante RACADM

Para cargar el certificado de servidor SSL, utilice el comando `sslcertupload`. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)* disponible en **dell.com/support/manuals**.

Carga de clave y certificado de Web Server

Es posible cargar una clave de Web Server y un certificado de servidor para la clave de Web Server. La autoridad de certificados (CA) emite el certificado de servidor.

El certificado de Web Server es un componente esencial que se utiliza en proceso de cifrado SSL. Se autentifica en un cliente habilitado 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 contar con 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, vaya a **Descripción general del chasis** y haga clic en **Red → SSL**. Aparecerá **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 **Aplicar**. Si la clave y el certificado de Web Server no coinciden, aparecerá un mensaje de error.

   NOTA: El CMC solo acepta certificados codificados con X509 base 64. No se aceptan los certificados que utilizan otros esquemas de codificación, como DER. Al cargar un nuevo certificado, se reemplaza el certificado predeterminado que se recibió con el CMC.

   Después de que el certificado se haya cargado correctamente, el CMC se reiniciará y no estará disponible temporalmente. Para evitar la desconexión de otros usuarios durante el restablecimiento, notifique a los usuarios autorizados que puedan tratar de iniciar sesión en el CMC y consulte la ficha **Red** de la página **Sesiones** para comprobar si existen sesiones activas.

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 <tipo> -f <nombre_de_archivo>
```

Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)* 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 del CMC, vaya a **Descripción general del chasis → Red → SSL**. Seleccione **Ver certificado del servidor** y haga clic en **Siguiente**. La página **Ver certificado del servidor** muestra el certificado SSL del servidor que está en uso. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

NOTA: El certificado del servidor mostrará el nombre común como el 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 del servidor SSL, utilice el comando `sslcertview`. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en **dell.com/support/manuals**.

Configuración de varios CMC mediante RACADM

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

Cuando se realiza una consulta en una tarjeta de CMC específica con las identificaciones de grupo y de objeto de la tarjeta, RACADM crea el archivo de configuración racadm.cfg a partir de la información obtenida. Mediante la exportación del archivo a uno o varios CMC, es posible configurar las controladoras con propiedades idénticas en una cantidad de tiempo mínima.

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

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

NOTA: El archivo de configuración generado es **myfile.cfg**. Es posible cambiar el nombre de archivo. El archivo **.cfg** no contiene contraseñas de usuario. Cuando el archivo **.cfg** se carga al CMC nuevo, es necesario volver a agregar todas las contraseñas.

2. Abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba:
   ```
   racadm getconfig -f myfile.cfg
   ```

   NOTA: El redireccionamiento de la configuración del CMC hacia un archivo por medio de `getconfig -f` solo se admite con la interfaz de RACADM remoto.

3. Modifique el archivo de configuración con un editor de texto 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 recientemente creado para modificar un CMC de destino. En el símbolo del sistema, escriba:
   ```
   racadm config -f myfile.cfg
   ```

5. Restablezca el 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 CMC para el CMC activo y genera el archivo **myfile.cfg**. Si es necesario, se puede cambiar el nombre de archivo o guardar el archivo 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 otros CMC. Server Administrator utiliza el comando `config` para sincronizar las bases de datos de usuarios y de contraseñas.

Enlaces relacionados

Creación de un archivo de configuración del CMC

Creación de un archivo de configuración del CMC

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

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

NOTA: Para obtener más información sobre el subcomando `getconfig`, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

RACADM analiza el archivo **.cfg** cuando se carga por primera vez en el CMC para verificar que los nombres de los grupos y los objetos presentes sean válidos y que se sigan ciertas reglas de sintaxis simples. Los errores se señalan con el número de la línea en la que se detectó el error y un mensaje explica el problema. El archivo completo se analiza para asegurar que sea correcto y se muestran todos los errores. Los comandos de escritura no se transmiten al CMC si se encuentra un error en el archivo **.cfg**. El usuario debe corregir todos los errores antes de poder realizar cualquier configuración.

Para verificar si existen errores antes de crear el archivo de configuración, utilice la opción `–c` con el subcomando `config`. Con la opción `–c`, `config` solo verifica la sintaxis y no escribe en el 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 del CMC para ese grupo. Todos los objetos dentro de ese grupo son modificaciones cuando el CMC se configura. Si un objeto modificado representa un índice nuevo, el índice se crea en el 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 existe un índice presente, se modifica ese índice. Si no existe un índice presente, se utiliza el primer índice disponible.

  Este método ofrece flexibilidad cuando se agregan anotaciones indexadas en las que no es necesario establecer correspondencias exactas del índice entre todos los CMC que se administran. Se agregan nuevos usuarios al primer índice disponible. Es posible que un archivo **.cfg** que se analiza y se ejecuta correctamente en un CMC no funcione correctamente en otro si todos los índices están llenos y se debe agregar un usuario nuevo.
- Use el subcomando `racresetcfg` para configurar ambos CMC con propiedades idénticas.

  Use el subcomando `racresetcfg` para restablecer el CMC a la configuración predeterminada original y, a continuación, ejecute el comando `racadm config -f <nombre_de_archivo>.cfg`. Asegúrese de que el archivo **.cfg** incluya todos los objetos, usuarios, índices y otros parámetros deseados. Para obtener una lista completa de los objetos y los grupos, consulte el capítulo sobre propiedades de la base de datos en *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

  PRECAUCIÓN: Use el subcomando `racresetcfg` para restablecer la base de datos y la configuración de la interfaz de red del CMC a sus valores predeterminados originales, y quite todos los usuarios y las configuraciones de usuario. Mientras el usuario raíz se encuentra disponible, los valores de configuración de los otros usuarios también se restablecen a los valores predeterminados.
- Si escribe `racadm getconfig -f <nombre_de_archivo>.cfg`, el comando genera un archivo **.cfg** para la configuración actual del CMC. Este archivo de configuración se puede usar como un ejemplo y como punto de inicio para el archivo **.cfg** único.

Enlaces relacionados

Reglas de análisis

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. Los caracteres "#" que se encuentren en cualquier otra columna se tratarán como caracteres #.

  Algunos parámetros de módem pueden incluir caracteres # en sus cadenas. No se requiere un carácter de escape. Se recomienda generar un archivo **.cfg** a partir de un comando `racadm getconfig -f <filename>.cfg` y, a continuación, ejecutar un comando `racadm config -f <filename>.cfg` para otro CMC, 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 inicial "[" que denota un nombre de grupo debe estar en la columna uno. Este nombre de grupo se debe especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado generan un error. Los datos de configuración se organizan en grupos tal y como se define en el capítulo de propiedad de base de datos de *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía

de referencia de la línea de comandos RACADM de iDRAC6 y CMC). El siguiente ejemplo muestra un nombre de grupo, un objeto y el valor de propiedad de ese objeto:

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

- Todos los parámetros se especifican como pares "objeto=valor" sin espacios en blanco entre el objeto, el símbolo "=" y el valor. Se ignorarán los espacios en blanco que se incluyan después del valor. Los espacios en blanco dentro de una cadena de valores se mantendrán sin modificación. Cualquier carácter que se encuentre a la derecha del signo = (por ejemplo, un segundo signo =, #, [,], etc.) se tomará tal como se encuentre. Estos caracteres son caracteres de secuencia de comandos de conversación de módem válidos.

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

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

  El usuario no puede especificar el índice que se debe utilizar. Si el índice ya existe, se utiliza ese o se crea la nueva anotación en el primer índice disponible de dicho grupo.

  El comando `racadm getconfig -f <filename>.cfg` coloca un comentario frente a los objetos de índice, lo que permite ver los comentarios incluidos.

  NOTA: Es posible crear un grupo indexado manualmente mediante el siguiente comando:

  ```
  racadm config -g <groupname> -o <anchored object> -i <index 1-16> <unique anchor name>
  ```

- La línea de un grupo indexado no se puede eliminar de un archivo **.cfg**. Si se elimina la línea con un editor de texto, RACADM se detendrá al analizar el archivo de configuración y generará una alerta sobre el error.

  El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

  ```
  racadm config -g <groupname> -o <objectname> -i <index 1-16> ""
  ```

  NOTA: Una cadena NULA (que se identifica con dos caracteres ") indica al CMC que elimine el índice para el grupo especificado.

  Para ver el contenido de un grupo indexado, utilice el siguiente comando:

  ```
  racadm getconfig -g <groupname> -i <index 1-16>
  ```

- Para los grupos indexados, el ancla del objeto debe ser el primer objeto después del par [ ]. A continuación se proporcionan ejemplos de grupos indexados actuales:

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

- Al usar RACADM remoto para capturar los grupos de configuración en un archivo, si no está configurada una propiedad clave dentro del grupo, el grupo de configuración no se guardará como parte del archivo de configuración. Para replicar estos grupos de configuración en otros CMC, configure la propiedad clave antes de ejecutar el comando `getconfig -f`. De manera alternativa, puede introducir manualmente las propiedades que faltan en el archivo mediante la ejecución del comando `getconfig -f`. Esto sucede en 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 del CMC en el archivo de configuración, quite todas las anotaciones `<variable> = <valor>` innecesarias. Solo la etiqueta del grupo de variables real con [y] permanece, incluidas las dos anotaciones `<variable> = <valor>` que pertenecen al cambio de dirección IP.

Ejemplo:

```
# # Object Group "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.10.110 cfgNicGateway=10.35.10.1
```

Este archivo se actualiza de la siguiente forma:

```
# # Object Group "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.9.143 # comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

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

Use este archivo para descargar cambios aplicables a toda la empresa o para configurar nuevos sistemas en la red con el comando `racadm getconfig -f <mi_archivo>.cfg`.

NOTA: *Anchor* es una palabra reservada y no se debe utilizar en el archivo **.cfg**.

Visualización y terminación de sesiones en el CMC

Puede ver el número de usuarios actualmente conectados en el iDRAC7 y terminar las sesiones de usuario.

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

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

Para ver o terminar una sesión mediante la interfaz web:

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Red → Sesiones**.
   La página **Sesiones** muestra el ID de la sesión, el nombre de usuario, la dirección IP y el tipo de sesión. Para obtener más información acerca de estas propiedades, consulte *CMC Online Help (Ayuda en línea para el 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 actual, utilice el comando `getssninfo`.

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

Para obtener más información sobre estos comandos, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)* disponible en **dell.com/support/manuals**.

7

Configuración del servidor

Es posible realizar las siguientes acciones para 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

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).
- Los nombres de las ranuras deben ser únicos dentro del chasis. Dos ranuras no pueden tener el mismo nombre.
- Las cadenas no distinguen entre mayúsculas y minúsculas. `Servidor-1, servidor-1 y SERVIDOR-1` son nombres equivalentes.
- Los nombres de las ranuras no deben comenzar con las siguientes cadenas:
  - `Conmutador-`
  - `Ventilador-`
  - `PS-`
  - `KVM`
  - `DRAC-`
  - `MC-`
  - `Chasis`
  - `Cubierta-Izquierda`
  - `Cubierta-Derecha`
  - `Cubierta-Central`
- Se pueden utilizar las cadenas `Servidor-1` a `Servidor-16`, pero solo para la ranura correspondiente. Por ejemplo, `Servidor-3` es un nombre válido para la ranura 3, pero no para la ranura 4. Observe que `Servidor-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**.

El valor de cada nombre de ranura en la interfaz web reside en el CMC solamente. Si se quita un servidor del chasis, el valor del nombre de ranura no permanece en el servidor.

El valor de cada nombre de ranura no se extiende al iKVM opcional. La información de nombre de ranura 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 **Descripción general del chasis** → **Descripción general del servidor** y haga clic en **Configuración** → **Nombres de las ranuras**. Aparecerá la página **Nombres de las ranuras**.
2. En el campo **Nombre de ranura**, edite el nombre de la ranura. Repita este paso para cada ranura cuyo nombre desee cambiar.
3. Para usar el nombre de host del servidor como nombre de ranura, seleccione **Utilizar nombre de host** para la opción **Nombre de ranura**. Esto suprime los nombres de ranura estáticos con el nombre de host del servidor (o el nombre del sistema), si se encuentra disponible. Se requiere que el agente OMSA esté instalado en el servidor. Para obtener más información sobre el agente OMSA, consulte *Dell OpenManage Server Administrator User's Guide* (Guía del usuario de Dell OpenManage Server Administrator).
4. Haga clic en **Aplicar** para guardar la configuración.
5. 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

Es posible determinar la configuración de red del 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 del iDRAC y la contraseña raíz para los servidores que se instalen posteriormente; esta configuración predeterminada es la configuración de QuickDeploy para el iDRAC.

Para obtener más información sobre el iDRAC, consulte *iDRAC7 User's Guide (Guía del usuario del iDRAC7)* en **dell.com/support/manuals**.

Enlaces relacionados

Configuración de los valores de red de QuickDeploy del iDRAC
Modificación de la configuración de red del iDRAC en un servidor individual
Modificación de la configuración de red del iDRAC mediante RACADM

Configuración de los valores de red de QuickDeploy del iDRAC

Use los valores de QuickDeploy para configurar los valores de red de los servidores recién insertados. Después de activar QuickDeploy, sus valores se aplican a los servidores cuando se instala ese servidor.

Para activar y establecer los valores de QuickDeploy del iDRAC mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **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 13. : Configuración de QuickDeploy

Configuración	Descripción
QuickDeploy activada	Activa o desactiva la función **QuickDeploy** que aplica automáticamente los valores del iDRAC configurados en esta página en los servidores recién insertados; la configuración automática debe confirmarse localmente en el panel LCD.

Configuración	Descripción
	NOTA: Esto incluye la contraseña de usuario raíz si se selecciona la casilla **Definir contraseña raíz al insertar servidor**. De manera predeterminada, esta opción está desactivada.
Activar implementación de perfiles del servidor	Activa la implementación de perfiles en servidores recientemente insertados después de la confirmación en el panel LCD, siempre que los perfiles estén asignados a la ranura en la página **Perfiles**.
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 **Definir contraseña raíz del iDRAC al insertar servidor** y **QuickDeploy activada**, este valor de contraseña se asigna a la contraseña de usuario raíz del iDRAC de un servidor cuando se inserta el servidor en el chasis. La contraseña puede tener de 1 a 20 caracteres imprimibles (incluyendo 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 de LAN del iDRAC. De forma predeterminada, esta opción está desactivada.
Activar IPv4 del iDRAC	Activa o desactiva IPv4 en el iDRAC. De forma predeterminada, esta opción está activada.
Activar la IPMI en la LAN del iDRAC	Activa o desactiva IPMI en el canal de LAN para cada iDRAC presente en el chasis. De forma predeterminada, esta opción está desactivada.
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 para cada iDRAC. De forma predeterminada, esta opción está desactivada.
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.

Configuración	Descripción
	NOTA: La máscara de subred y la puerta de enlace no se incrementan como la dirección IP. Por ejemplo, si la dirección IP inicial es `192.168.0.250` y la máscara de subred es `255.255.0.0`, la dirección IP de QuickDeploy para la ranura 15 es `192.168.0.265`. Si la máscara de subred fuera `255.255.255.0`, se muestra el mensaje de error `QuickDeploy IP address range is not fully within QuickDeploy Subnet` (El rango de direcciones IP de QuickDeploy no se encuentra completamente dentro de la subred de QuickDeploy) al hacer clic en **Guardar configuración de QuickDeploy** o **Completar automáticamente con la configuración de QuickDeploy**.
Máscara de red IPv4 del iDRAC	Especifica la máscara de subred de QuickDeploy que se asigna a todos los servidores recién insertados.
Puerta de enlace IPv4 del iDRAC	Especifica la puerta de enlace predeterminada de QuickDeploy que se asigna a todos los 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.

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 se seleccionan **Definir contraseña raíz del iDRAC al insertar servidor** y **QuickDeploy activada**, se pedirá al usuario que utilice la interfaz LCD para permitir o impedir el cambio de la contraseña. Si existen valores de configuración de red que difieren de la configuración actual del iDRAC, se le pide al usuario que acepte o rechace los cambios.

   NOTA: Cuando existe una diferencia de LAN o IPMI en LAN, el sistema le solicita al usuario que acepte el valor de dirección IP de QuickDeploy. Si la diferencia es el valor 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 para los cambios realizados en uno o más valores de configuración de red del servidor iDRAC se necesiten varios minutos para que se propaguen del CMC al iDRAC. Si se hace clic en **Actualizar** sin esperar unos minutos, es posible que se muestren solo los datos parcialmente correctos para uno o más servidores iDRAC.

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

Con esta tabla, se pueden definir los valores de configuración de red del iDRAC para cada servidor instalado. Los valores iniciales que se muestran para cada uno de los campos son los valores actuales que se leen en el iDRAC.

Para modificar la configuración de red del iDRAC mediante la interfaz web del CMC:

1. En el árbol del sistema, vaya a **Descripción general del servidor** y haga clic en **Configuración → iDRAC**. Aparecerá la página **Implementar iDRAC**. La sección **Configuración de red del iDRAC** muestra todos los valores de configuración de red IPv4 e IPv6 para el iDRAC de los servidores instalados.
2. Modifique la configuración de red del iDRAC según sea necesario para los servidores.

   NOTA: Es necesario seleccionar la opción **Activar LAN** para especificar la configuración de IPv4 o IPv6. Para obtener información sobre estos campos, consulte CMC Online Help (Ayuda en línea para el CMC).
3. Para implementar la configuración en el iDRAC, haga clic en **Aplicar configuración de red del iDRAC**. Si realizó algún cambio en la configuración de QuickDeploy, eso también se guardará.

   La tabla **Configuración de red del iDRAC** refleja los valores de configuración de red futuros; los valores mostrados para los servidores instalados pueden o no ser los mismos valores de configuración de red del iDRAC instalados actualmente. Haga clic en **Actualizar** para actualizar la página **Implementación del iDRAC** con cada valor de configuración de red del iDRAC instalado después de realizar los cambios.

   NOTA: Los cambios realizados en los campos de QuickDeploy son inmediatos, pero los cambios realizados en uno o varios valores de configuración de red del servidor iDRAC pueden requerir un par de minutos para propagarse del CMC a un iDRAC. Si se hace clic en **Actualizar** demasiado rápido, es posible que solo se muestren datos parcialmente correctos para uno o varios servidores iDRAC.

Modificación de la configuración de red del iDRAC mediante RACADM

Los comandos `config` o `getconfig` de RACADM admiten la opción `–m <módulo>` para los grupos de configuración siguientes:

- `[cfgLanNetworking]`
- `cfgIPv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

Para obtener más información sobre los valores y rangos predeterminados de propiedades, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC).

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.

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, vaya a **Descripción general del chasis** y haga clic en **Red** → **VLAN**.
   - En el árbol del sistema, vaya a **Descripción general del chasis** → **Descripción general del servidor** y haga clic en **Red** → **VLAN**. Aparecerá la página **Configuración de la etiqueta VLAN**.
2. En la sección **iDRAC**, active la red VLAN para los servidores, establezca la prioridad y especifique la identificación. Para obtener más información sobre los campos, consulte *CMC Online Help (Ayuda en línea para el 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 de 1 a 16.

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

  Los valores válidos para `<VLAN priority>` (<Prioridad de VLAN>) son de 0 a 7. El valor predeterminado es 0.

  Por ejemplo:
  ```
  racadm setniccfg –m server-1 –v 1 7
  ```
  Por ejemplo:
- Para eliminar la VLAN de un servidor, desactive las capacidades de VLAN de la red del servidor especificado:
  ```
  racadm setniccfg –m server-<n> –v
  ```
  Los valores válidos para `<n>` son de 1 a 16.

  Por ejemplo:
  ```
  racadm setniccfg –m server-1 –v
  ```

Configuración del primer dispositivo de inicio

El usuario puede especificar el primer dispositivo de inicio del CMC para cada servidor. Es posible que este no sea el primer dispositivo de inicio real para el servidor ni que represente un dispositivo presente en ese servidor, sino que represente un dispositivo que el CMC envía al servidor y se utiliza como el primer dispositivo de inicio con respecto a ese servidor.

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.

Es posible configurar el primer dispositivo de inicio para el siguiente inicio solamente o para todos los reinicios subsiguientes. Según esta selección, se puede establecer el primer dispositivo de inicio para el servidor. El sistema se iniciará desde el dispositivo seleccionado la próxima vez que se reinicie y todas las veces subsiguientes. Ese dispositivo seguirá siendo el primer dispositivo de inicio en el orden de inicio del BIOS hasta que se vuelva a cambiar en la interfaz web del CMC o en 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 14. : Dispositivos de inicio

Dispositivo de inicio	Descripción
PXE	Inicio a partir de un protocolo de entorno de ejecución previa al inicio (PXE) en la tarjeta de interfaz de red.
Unidad de disco duro	Inicio a partir del disco duro del servidor.
CD/DVD local	Inicio a partir de una unidad de CD/DVD en el servidor.
Disco flexible virtual	Inicio a partir de la unidad de disco flexible virtual. La unidad de disco flexible (o una imagen del disco flexible) se encuentra en otro equipo en la red de administración y se conecta a través del visor de consola de la interfaz gráfica de usuario del iDRAC.
CD/DVD virtual	Inicio a partir de una unidad de CD/DVD virtual o de una imagen ISO de CD/DVD. La unidad óptica o el archivo de imagen ISO se encuentra en otro equipo o disco disponible en la red de administración y se conecta a través del visor de consola de la interfaz gráfica de usuario del iDRAC.
iSCSI	Inicio a partir de un dispositivo de interfaz estándar de equipos pequeños (iSCSI) de Internet.
Tarjeta SD local	Inicio a partir de la tarjeta SD (Secure Digital) local, solo para servidores que admiten sistemas iDRAC6 e iDRAC7.
Disco flexible	Inicio a partir de un disco flexible en la unidad de disco flexible local.
RFS	Inicio a partir de una imagen de recurso compartido de archivos remotos (RFS). El archivo de imagen se adjunta mediante el visor de consola de la interfaz gráfica de usuario del iDRAC.

Enlaces relacionados

Configuración del primer dispositivo de inicio para varios servidores mediante la interfaz web del CMC
Configuración del primer dispositivo de inicio para un servidor individual mediante la interfaz web del CMC
Configuración del primer dispositivo de inicio mediante RACADM

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 **Descripción general del servidor** y haga clic en **Configuración → Primer dispositivo de inicio**. Se mostrará 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 se inicie desde el dispositivo seleccionado cada vez que se inicie, desactive la opción **Inicio único** para el servidor. Si desea que el servidor se inicie desde el dispositivo seleccionado solamente en el siguiente ciclo de inicio, active la opción **Inicio único** 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 **Configuración → Primer dispositivo de inicio**. Se mostrará la página **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 se inicie desde el dispositivo seleccionado cada vez que se inicie, desactive la opción **Inicio único** para el servidor. Si desea que el servidor se inicie desde el dispositivo seleccionado solamente en el siguiente ciclo de inicio, active la opción **Inicio único** 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 único de un dispositivo, utilice el objeto `cfgServerBootOnce`.

Para obtener más información sobre estos objetos, consulte *RACADM Command Line Reference Guide for iDRAC and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)* 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 **Remote Virtual Media File Share (Recurso compartido de archivos de medios virtuales remoto)** asigna un archivo de una unidad compartida en la red a uno o varios servidores mediante el CMC con el fin de implementar o actualizar un sistema operativo. Cuando se encuentra conectado, es posible obtener acceso al archivo remoto como si estuviera en el sistema local. Se admiten dos tipos de medios: unidades de disco flexible 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 algunos de los servidores presentes en las ranuras son de 12° generación o posterior y no tiene una licencia apropiada, aparece un mensaje que le indica que falta una licencia requerida o que está caducada. Debe obtener una licencia apropiada y volver a intentarlo o comuníquese con su proveedor de servicio para obtener más detalles.
2. Especifique los valores necesarios. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
3. Haga clic en **Conectar** para conectarse con un recurso compartido de archivos remoto. Para conectarse con un recurso compartido de archivos remoto, debe proporcionar la ruta de acceso, el nombre de usuario y la contraseña. Si la operación se realiza con éxito, se le permite obtener acceso 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 todas las opciones de perfil de un servidor especificado a uno o más servidores. Las opciones de perfil que pueden replicarse son las que pueden modificarse y están pensadas para replicarse en servidores. Se muestran los siguientes tres grupos de perfiles de servidores, que pueden replicarse:

- BIOS: este grupo incluye solo las opciones de BIOS de un servidor. Estos perfiles se generan desde las versiones del CMC anteriores a la 4.3.
- BIOS e inicio: este grupo incluye las opciones de BIOS y de inicio de un servidor. Estos perfiles se generan desde:
  - CMC versión 4.3
  - CMC versión 4.45 con servidores 11G
  - CMC versión 4.45 y servidores 12G con Lifecycle Controller 2 de una versión anterior a la 1.1
- Todas las opciones: esta versión incluye todas las opciones del servidor y los componentes en ese servidor. Estos perfiles se generan desde el CMC versión 4.45 y servidores 12G con iDRAC7 y Lifecycle Controller 2 versión 1.1 o superior.

La función de replicación de configuración de servidores admite los servidores iDRAC6 e iDRAC7. Los servidores RAC de generaciones anteriores se muestran en la lista pero aparecen en gris en la página principal y no están activados para usar esta función.

Para usar la función de replicación de configuración de servidores:

- iDRAC debe tener la versión mínima requerida. Los servidores iDRAC6 requieren, como mínimo, la versión 3.2 y los servidores iDRAC7 requieren la versión 1.00.00.
- El servidor debe estar encendido.

Versiones de servidores y compatibilidades de perfiles:

- iDRAC7 con Lifecycle Controller 2 versión 1.1 puede aceptar cualquier versión de perfil.
- iDRAC6 versión 3.2 e iDRAC7 con Lifecycle Controller 2 versión 1.0 solo acepta perfiles de BIOS o de BIOS e inicio.
- Guardar un perfil desde un servidor iDRAC7 con Lifecycle Controller 2 versión 1.1 resulta en un perfil de Todas las opciones. Guardar un perfil desde un servidor con iDRAC6 V3.2 e iDRAC7 con LC2V1 resultará en 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 un recurso compartido de archivos remotos.
- Editar el nombre y la descripción del perfil.
- Exportar los perfiles almacenados a 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.

Enlaces relacionados

Acceso a la página Perfiles de servidores
Agregar o guardar perfil
Aplicación de un perfil
Visualizar configuración de perfil
Visualización del registro de perfiles
Estado de compleción y solución de problemas

Acceso a la página Perfiles de servidores

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

Para acceder a la página **Perfiles de servidores** con la interfaz web del CMC, en el árbol del sistema, diríjase a **Descripción general del chasis** → **Descripción general del servidor** y haga clic en **Configuración** → **Perfiles**. Aparecerá la página **Perfiles de servidores**.

Enlaces relacionados

Agregar o guardar perfil
Aplicación de un perfil
Visualizar configuración de perfil
Visualización del registro de perfiles
Estado de compleción y solución de problemas

Agregar o guardar perfil

Antes de clonar las propiedades de un servidor, en primer lugar capture las propiedades en un perfil almacenado. Cree un perfil almacenado, 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 del CMC.

La eliminación o desactivación del soporte de almacenamiento extendido no volátil impide el acceso al perfil almacenado y desactiva la función Clonación de servidores.

Para agregar o guardar un perfil:

1. Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles del servidor**, seleccione el servidor desde cuya configuración desea generar el perfil y, a continuación, haga clic en **Guardar perfil**.

   Aparecerá la sección **Guardar perfil del servidor**.
2. En los campos **Nombre de perfil** y **Descripción** ingrese el nombre de perfil y la descripción (opcional) y haga clic en **Guardar perfil**.

   El CMC se comunica con el LC para obtener la configuración del perfil del servidor disponible y almacenarla como perfil designado.

   Un indicador de progreso determina si la operación Guardar está en curso. Una vez que se completó la acción, aparece un 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

Enlaces relacionados

Acceso a la página Perfiles de servidores

Aplicación de un perfil

La clonación de servidores solo es posible cuando existen perfiles de servidores disponibles como perfiles almacenados en el soporte no volátil del CMC. Para iniciar una operación de clonación 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 de servidores**. En la sección **Guardar y aplicar perfiles**, seleccione el o los servidores para los que desea aplicar el perfil seleccionado.

   Se activará el menú desplegable **Seleccionar perfil**.
2. En el menú desplegable **Seleccionar perfil**, seleccione el perfil que desea aplicar.

   Se activa la opción **Aplicar perfil**.
3. Haga clic en **Aplicar perfil**.

   Aparece un mensaje de aviso de que al aplicar un nuevo perfil de servidor se sobrescribirá la configuración actual y también se reiniciarán los servidores seleccionados. Se le pide que confirme si desea continuar con la operación.

   NOTA: Para realizar operaciones de clonación en servidores, la opción CSIOR debe estar activada para los servidores. Si esta opción está desactivada, aparecerá un mensaje de advertencia para notificar que CSIOR no está activado para los servidores. Para completar la operación de clonación de blade, asegúrese de activar la opción CSIOR para los servidores.

4. Haga clic en **Aceptar** para aplicar el perfil al servidor seleccionado.

   El perfil seleccionado se aplica a los servidores, que pueden reiniciarse de inmediato si es necesario. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Enlaces relacionados

Acceso a la página Perfiles de servidores

Importar archivo

Puede importar al CMC un perfil de servidor almacenado en un recurso compartido de archivos remotos.

Para importar al CMC un perfil almacenado en un recurso compartido de archivos remotos:

1. En la página **Perfiles de servidor**, dentro de la sección **Perfiles en la tarjeta SD**, 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 el soporte no volátil (tarjeta SD) del CMC a una ruta de acceso específica en un recurso compartido de archivos remotos.

Para exportar un perfil almacenado:

1. Diríjase a la página **Perfiles del servidor**. Dentro de la sección **Perfiles en la tarjeta SD**, 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.

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

Editar perfil

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

Para editar un perfil almacenado:

1. Diríjase a la página **Perfiles de servidores**. En la sección **Perfiles en la tarjeta SD**, seleccione el perfil requerido y haga clic en **Editar perfil**.

   Aparecerá la sección **Editar perfil de BIOS — <Nombre de perfil>**.

2. Edite el nombre y la descripción del perfil del servidor según sea necesario y luego haga clic en **Editar perfil**.

   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 el soporte no volátil del CMC (tarjeta de SD).

Para eliminar un perfil almacenado:

1. En la página **Perfiles del servidor**, dentro de la sección **Administrar perfiles en la tarjeta SD**, seleccione el perfil requerido y haga clic en **Eliminar perfil**.

Aparecerá un mensaje de aviso donde se indica que al eliminar un perfil se eliminará permanentemente el perfil seleccionado.

2. Haga clic en **Aceptar** para eliminar el perfil seleccionado.
   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

Visualizar configuración de perfil

Para ver la **Configuración de perfil** de un servidor seleccionado, diríjase a la página **Perfiles del servidor**. En la sección **Perfiles del servidor**, haga clic en **Ver** en la columna **Perfil del servidor** del servidor requerido. Aparecerá 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 la opción 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.

Enlaces relacionados

Acceso a la página Perfiles de servidores

Visualización de la configuración de los perfiles almacenados

Para ver la configuración de los perfiles de servidores almacenados en el soporte no volátil (tarjeta de SD) del CMC, diríjase a la página **Perfiles del servidor**. En la sección **Perfiles en la tarjeta SD**, haga clic en **Ver** en la columna **Ver perfil** del servidor requerido. Aparecerá 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**. Esta sección enumera las 10 entradas más recientes del registro de perfiles directamente desde las operaciones de clonación de servidores. Cada entrada del registro muestra la gravedad, la fecha y la hora de envío de la operación de clonación de servidores y la descripción del mensaje de registro de clonación. 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)*.

Estado de compleción 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 **Descripción general del servidor** y haga clic en **Solución de problemas** → **Trabajos de Lifecycle Controller**. Busque la misma JID en la tabla **Trabajos**.

Implementación rápida de perfiles

La función Implementación rápida le permite asignar un perfil almacenado a una ranura de servidor. Cualquier servidor compatible con la creación de copias idénticas de servidores insertado en esa ranura se configurará con el perfila asignado. Puede realizar la acción de Implementación rápida solo si la opción **Activar implementación de perfiles del servidor** está activada en la página **Implementar iDRAC**. Para ir a la página **Implementar iDRAC**, seleccione **Descripción general de servidor → Configuración → iDRAC**. Los perfiles que pueden implementarse están incluidos en la tarjeta SD.

NOTA:

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

Asignación de perfiles del servidor a ranuras

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

1. En la página **Perfiles del servidor**, diríjase a la sección **Perfiles para implementación rápida**.
   Aparecerán las asignaciones de perfiles actuales para las ranuras en los cuadros seleccionados en la columna **Perfil del servidor**.
2. En la lista desplegable, seleccione el perfil que desea asignar a la ranura requerida. Puede seleccionar perfiles para aplicar a varias ranuras.
3. Haga clic en **Asignar**.
   Se aplicarán los perfiles 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.

NOTA: Para quitar todas las asignaciones de perfiles de una ranura, seleccione **Sin perfil seleccionado** en la lista desplegable.

NOTA: Cuando se implementa un perfil en un servidor con la función **Perfil para implementación rápida**, el progreso y los resultados de la aplicación se conservan en el registro de perfiles.

Inicio del iDRAC mediante el inicio de sesión único

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

Un usuario puede iniciar la interfaz web del iDRAC sin tener que iniciar sesión por segunda vez, ya que esta función utiliza el inicio de sesión único. Las políticas de inicio de sesión único son:

- Un usuario del CMC con el privilegio de administración del servidor se conectará automáticamente con el iDRAC mediante el inicio de sesión único. Una vez que este usuario se encuentre en el sitio del iDRAC, se le otorgarán privilegios de administrador automáticamente. Esto sucede incluso cuando el usuario no dispone de una cuenta en el iDRAC o la cuenta no tiene privilegios de administrador.
- Un usuario del CMC **SIN** el privilegio de administración del servidor, pero con la misma cuenta en el iDRAC, se conectará automáticamente con el iDRAC mediante el inicio de sesión único. Una vez que este usuario se encuentre en el sitio del iDRAC, se le otorgarán privilegios que fueron creados para la cuenta del iDRAC.
- Un usuario del CMC sin el privilegio de administración del servidor o la misma cuenta en el iDRAC, **NO** se conectará automáticamente con el iDRAC mediante el inicio de sesión único. Este usuario será dirigido a la página de inicio de sesión del iDRAC al hacer clic en el botón **Iniciar interfaz gráfica de usuario del iDRAC**.

NOTA: En este contexto, el término "la misma cuenta" significa que el usuario tiene el mismo nombre de inicio de sesión con una contraseña que coincide para el CMC y para el iDRAC. Cuando el usuario tenga el mismo nombre de inicio de sesión pero no disponga de una contraseña que 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 se extrae el servidor del chasis, se cambia la dirección IP del iDRAC o la conexión de red del iDRAC tiene algún problema, es posible que aparezca una página de error al hacer clic en Iniciar interfaz gráfica de usuario del iDRAC.

Enlaces relacionados

Inicio del iDRAC desde la página Estado de los servidores
Inicio del iDRAC desde la página Estado del servidor

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 **Descripción general del servidor**. Se mostrará 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 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 **Descripción general del servidor**. Todos los servidores (de 1 a 16) aparecerán en la lista expandida **Servidores**.
2. Haga clic en el servidor para el que desea iniciar la interfaz web del iDRAC. Aparecerá la página **Estado del servidor**.
3. Haga clic en **Iniciar interfaz gráfica de usuario del iDRAC**. Aparecerá la interfaz web del iDRAC.

Inicio de la consola remota desde la interfaz web del CMC

Es posible iniciar una sesión de KVM (teclado, video y mouse) directamente en el servidor. La función de consola remota solo se admite cuando se cumplen todas las siguientes condiciones:

- El chasis está encendido.
- Los servidores admiten iDRAC6 e iDRAC7.
- 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 del iDRAC. Para obtener más detalles, consulte *iDRAC User's Guide (Guía del usuario del iDRAC)*.

Enlaces relacionados

Inicio de la consola remota desde la página Condición del chasis
Inicio de la consola remota desde la página Estado del servidor

Inicio de la consola remota desde la página Estado de los servidores

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, vaya a **Descripción general del chasis** y haga clic en **Propiedades** → **Condición**. Aparecerá la página **Condición 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

Es posible configurar alertas y acciones para ciertos sucesos que se producen en el sistema administrado. Se produce un suceso cuando el estado de un componente del sistema supera la condición predefinida. Si un suceso coincide con un filtro de suceso y ese filtro se ha configurado para generar una alerta (alerta por correo electrónico o captura SNMP), se envía una alerta a uno o varios de los destinos configurados.

Para configurar el 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.

Enlaces relacionados

Activación o desactivación de alertas
Configuración de destinos de alerta

Activación o desactivación de alertas

Para enviar alertas a los destinos configurados, debe activar la opción de alerta global. Esta propiedad anula la configuración de la alerta individual.

Asegúrese de que el SNMP o los destinos de alerta por correo electrónico estén configurados para recibir las alertas.

Activación o desactivación de alertas mediante la interfaz web del CMC

Para activar o desactivar la generación de alertas:

1. En el 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, desactive 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 **Activar alerta** en el encabezado de columna para generar alertas para todos los sucesos. De otro modo, desactive esta opción.
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 RACAM **cfgIpmiLanAlertEnable**. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

Configuración de destinos de alerta

La estación de administración utiliza el protocolo simple de administración de red (SNMP) para recibir datos del 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**.

Enlaces relacionados

Configuración de destinos de alerta de las capturas SNMP

Configuración de los valores de alertas por correo electrónico

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 **Destino**, especifique una dirección IP válida. Utilice el formato IPv4 de cuatro números con puntos intermedios, la notación estándar de dirección IPv6 o el nombre de dominio completo (FQDN). Por ejemplo: **123.123.123.123** o **2001:db8:85a3::8a2e:370:7334** o **dell.com**.
     Elija un formato que sea consistente con la infraestructura o la tecnología de red. La función Probar captura no puede detectar las elecciones incorrectas en función de la configuración de red (por ejemplo, el uso de un destino IPv6 en un entorno exclusivamente de IPv4).
   - En el campo **Cadena de comunidad**, especifique una cadena de comunidad válida a la que pertenezca la estación de administración de destino.
     Esta cadena de comunidad es distinta a la que se muestra en la página **Chasis** → **Red** → **Servicios**. La cadena de comunidad de capturas SNMP es la comunidad que CMC utiliza para las capturas de salida destinadas a las estaciones de administración. La cadena de comunidad de la página **Chasis** → **Red** → **Servicios** es la cadena de comunidad que las estaciones de administración utilizan para consultar el daemon SNMP en el CMC.
   - En **Activada**, seleccione la casilla correspondiente a la dirección IP de destino para activar la dirección IP de forma que reciba las capturas. Es posible especificar hasta cuatro direcciones IP.
3. Haga clic en **Aplicar** para guardar la configuración.
4. Para probar si la dirección IP puede recibir las capturas SNMP, haga clic en **Enviar** en la columna **Probar captura SNMP**.
   Se configurarán los destinos de alerta IP.

Configuración de destinos de alerta de las capturas SNMP mediante RACADM

Para configurar los destinos de alerta IP mediante RACADM:

1. Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.

NOTA: Solo se puede seleccionar una máscara de filtro para las alertas tanto de SNMP como por correo electrónico. Es posible ignorar el paso 2 si ya se 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>` (<valor de máscara>) 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 capturas para el aviso de sonda de baterías (0x2), la falla del suministro de energía (0x1000) y la falla del KVM (0x80000), escriba: 2 <OR> 1000 <OR> 80000 y presione la tecla <=>.

   El valor hexadecimal resultante es 81002, y el valor de la máscara para el comando RACADM es 0x81002.

Tabla 15. 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

Suceso	Valor de la máscara de filtro
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> (<índice>) es un valor entre 1 y 4. El 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> (<dirección IP>) es un destino válido y <index> (<índice>) es el valor de índice que se especificó en el paso 4.

6. Especifique el nombre de comunidad:
   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i
   <index>
   ```
   donde <community name> (<nombre de comunidad>) es la comunidad SNMP a la que pertenece el chasis e <index> (<índice>) es el valor de índice que se especificó en los pasos 4 y 5.

   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 que se ha especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgTraps -i <index>`. Si el índice está configurado, aparecerán los valores para los objetos **cfgTrapsAlertDestIPAddr** y **cfgTrapsCommunityName**.

7. Para probar cuál es el destino de las alertas de una captura de sucesos, escriba:
   ```
   racadm testtrap -i <index>
   ```
   donde <index> (<índice>) es un valor de 1 a 4 que representa el destino de alerta que desea probar.

   Si no sabe con seguridad cuál es el número de índice, use:
   ```
   racadm getconfig -g cfgTraps -i <index>
   ```

Configuración de los valores de 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.

Es necesario configurar el servidor de correo electrónico SMTP para aceptar correos electrónicos retransmitidos de la dirección IP del CMC, una función que normalmente está desactivada en la mayoría de los servidores de correo electrónico por motivos de seguridad. Para obtener instrucciones acerca de cómo realizarlo de forma segura, consulte la documentación incluida con el servidor SMTP.

NOTA: Si el servidor de correo es Microsoft Exchange Server 2007, compruebe que el nombre de dominio de iDRAC7 está configurado para que el servidor de correo reciba alertas por correo electrónico desde iDRAC7.

NOTA: Las alertas por correo electrónico admiten direcciones IPv4 e IPv6. El nombre de dominio DNS de DRAC se debe especificar mediante IPv6.

Si la red tiene un servidor SMTP que genera y renueva las concesiones de las direcciones IP periódicamente, y las direcciones son distintas, habrá un período durante el cual el valor 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 sobre los campos, consulte *CMC Online Help (Ayuda en línea para el 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 con RACADM:

1. Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
2. Active la generación de alertas:
   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
   NOTA: Solo se puede seleccionar una máscara de filtro para las alertas tanto de SNMP como por correo electrónico. Si ya ha establecido una máscara de filtro, puede omitir el paso 3.
3. Especifique los sucesos para los que se deben generar alertas:
   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
   ```
   donde `<mask value>` (<valor de máscara>) es un valor hexadecimal entre 0x0 y 0xffffffff que se debe expresar con los caracteres iniciales 0x. En la tabla Máscaras de filtro para capturas de sucesos se proporcionan máscaras de filtro para cada tipo de suceso. Para obtener instrucciones acerca de la forma de calcular el valor hexadecimal para la máscara de filtro que desea activar, consulte el paso 3 en Configuring SNMP Trap Alert Destinations Using RACADM (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>` (<índice>) es un valor entre 1 y 4. El CMC utiliza 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>` (<dirección de correo electrónico>) es una dirección de correo electrónico válida e `<index>` (<índice>) es el valor del índice que se especificó en el paso 4.
6. Especifique el nombre de la persona que recibirá la alerta por correo electrónico:
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i
   <index>
   ```
   donde `<email name>` (<nombre de correo electrónico>) es el nombre de la persona o el grupo que recibirá la alerta por correo electrónico e `<index>` (<índice>) es el valor del índice que se especificó 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` (host.dominio) 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 que se ha especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgEmailAlert — I <index>`. Si el índice está configurado, aparecerán los valores para los objetos **cfgEmailAlertAddress** y **cfgEmailAlertEmailName**.

   Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) disponible en **dell.com/support/manuals**.

9

Configuración de cuentas de usuario y privilegios

Es posible configurar las cuentas de usuario con privilegios específicos (*autoridad basada en funciones*) para administrar el sistema mediante el CMC y mantener la seguridad del sistema. De manera predeterminada, el CMC está configurado con una cuenta de administrador local. Este nombre de usuario predeterminado es *root* y la contraseña es *calvin*. Como administrador, es posible configurar cuentas de usuario para permitir a otros usuarios obtener acceso al CMC.

Es posible configurar hasta 16 usuarios locales o utilizar servicios de directorio, como Microsoft Active Directory o LDAP, para configurar cuentas de usuario adicionales. El uso de un servicio de directorio proporciona una ubicación central para administrar las cuentas de usuario autorizadas.

El CMC admite el acceso basado en funciones para los usuarios con un conjunto de privilegios asociados. Las funciones son: administrador, operador, solo lectura o ninguno. La función define los privilegios máximos disponibles.

Enlaces relacionados

Tipos de usuarios
Configuración de usuarios locales
Configuración de usuarios de Active Directory
Configuración de los usuarios LDAP genéricos
Modificación de la configuración de cuentas raíz de administración para usuarios

Tipos de usuarios

Hay dos tipos de usuarios:

- Usuarios del 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 del CMC pueden ser usuarios locales o usuarios del servicio de directorio.

Excepto cuando un usuario del CMC tiene privilegios de **Server Administrator**, los privilegios otorgados a un usuario del CMC no se transfieren automáticamente al mismo usuario en un servidor, ya que los usuarios del servidor se crean independientemente de los usuarios del CMC. En otras palabras, los usuarios de Active Directory del CMC y los usuarios de Active Directory del iDRAC residen en dos ramas diferentes del árbol de Active Directory. Para crear un usuario del servidor local, los usuarios de configuración deben conectarse directamente al servidor. Estos usuarios no pueden crear un usuario del servidor desde CMC ni viceversa. Esta regla protege la seguridad y la integridad de los servidores.

Tabla 16. : Tipos de usuarios

Privilegio	Descripción
Usuario con acceso al CMC	El usuario puede iniciar sesión en el CMC y ver todos los datos del CMC, pero no puede agregar o modificar datos ni ejecutar comandos. Es posible que un usuario tenga otros privilegios sin el privilegio de Usuario con acceso al CMC. Esta función es útil cuando no se le permite iniciar sesión temporalmente a un usuario. Cuando el privilegio de Usuario con

Privilegio	Descripción
	acceso al 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 del CMC. • Se relacionan con el chasis, como el nombre de ranura y la prioridad de ranura. Aunque estas propiedades se aplican a los servidores, se trata estrictamente de propiedades del chasis que se relacionan con las ranuras y no con los servidores en sí. Por este motivo, los nombres y las prioridades de ranura se pueden agregar o cambiar sin importar si los servidores están presentes en las ranuras. Cuando un servidor se mueve a otro chasis, hereda el nombre de ranura y la prioridad asignada a la ranura correspondiente en el nuevo chasis. El nombre y la prioridad de ranura anteriores se conservan en el chasis anterior. **NOTA:** Los usuarios del CMC que tienen el privilegio de **Administrador de configuración del chasis** pueden configurar los valores de alimentación. Sin embargo, el privilegio de **Administrador de control del chasis** es necesario para realizar operaciones de alimentación del chasis, como el encendido, el apagado y el ciclo de encendido.
Administrador de configuración de usuarios	El usuario puede: • Agregar un nuevo usuario. • Cambiar la contraseña de un usuario. • Cambiar los privilegios de un usuario. • Activar o desactivar el privilegio de inicio de sesión de un usuario, pero conservar el nombre del usuario y otros privilegios en la base de datos.
Administrador de borrado de registros	El usuario puede borrar los registros de hardware y del CMC.
Administrador de control del chasis (comandos de alimentación)	Los usuarios del CMC con privilegios de **Administrador de alimentación del chasis** pueden realizar todas las operaciones relacionadas con la administración de 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**.
Server Administrator	Se trata de un privilegio general que otorga al usuario del CMC todos los derechos para realizar cualquier operación en los servidores que estén presentes en el chasis. Cuando un usuario con el privilegio de **Server Administrator** genera una acción que se debe realizar en un servidor, el firmware del CMC envía el comando al servidor de destino sin verificar los privilegios del usuario en el servidor. Es decir, el privilegio de **Server Administrator** anula la falta de privilegios de administrador en el servidor.

Privilegio	Descripción
	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 del CMC que no tiene privilegios de **Server Administrator** genera una acción que se debe ejecutar en un servidor, el CMC envía un comando al servidor de destino con el nombre y la contraseña de inicio de sesión del usuario. Si el usuario no existe en el servidor o la contraseña no coincide, se negará al usuario la capacidad de ejecutar la acción. Si el usuario existe en el servidor de destino y la contraseña coincide, el servidor responderá según los privilegios que el usuario tenga en el servidor. En función de los privilegios que se tengan en el servidor, el firmware del CMC decidirá si el usuario tiene derecho de ejecutar la acción. A continuación se muestra una lista de los privilegios y las acciones en el servidor a los que se tiene derecho con el privilegio de Server Administrator. Estos derechos se aplican únicamente cuando el usuario del chasis no tiene privilegios de Administrador 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.

Privilegio	Descripción
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 del CMC proporcionan una serie de grupos de usuarios que tienen privilegios de usuario previamente asignados.

NOTA: Si selecciona Administrador, Usuario avanzado o Usuario invitado y, a continuación, agrega o elimina un privilegio del conjunto predefinido, la opción Grupo del CMC cambia automáticamente a Personalizado.

Tabla 17. : Privilegios del grupo del CMC

Grupo de usuarios	Privilegios otorgados
Administrador	• Usuario con acceso al CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Server Administrator • 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 • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Server Administrator • 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 al CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Server Administrator • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A • Administrador de red Fabric B

Grupo de usuarios	Privilegios otorgados
	• Administrador de red Fabric C
Ninguno	Sin permisos asignados

Tabla 18. Comparación de los privilegios entre administradores, usuarios avanzados y usuarios invitados del CMC

Conjunto de privilegios	Permisos de administrador	Permisos de usuario avanzado	Permisos de usuario invitado
Usuario con acceso al 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
Server Administrator	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 raíz (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.

   Se muestra 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 **Apply (Aplicar)**.
   Se cambiará la contraseña para la identificación de usuario 1.

Configuración de usuarios locales

Es posible configurar hasta 16 usuarios locales en el CMC con permisos de acceso específicos. Antes de crear un usuario local para el CMC, compruebe si existen usuarios actuales. Puede establecer nombres de usuario, contraseñas y funciones con privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar mediante cualquiera de las interfaces seguras del 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 el CMC:

NOTA: Es necesario contar con el permiso **Configurar usuarios** para poder crear un usuario 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 un número de identificación 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.

   Se muestra 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 **Apply (Aplicar)**.
   El usuario se creará 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.

Es posible configurar hasta 16 usuarios en la base de datos de propiedades del CMC. Antes de activar manualmente un usuario del CMC, verifique si existe algún usuario actual.

Si desea configurar un nuevo CMC o si ha usado el comando racadm `racresetcfg`, el único usuario actual es `root` con la contraseña `calvin`. El subcomando `racresetcfg` restablece todos los parámetros de configuración a los valores 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 del CMC.

Varios parámetros e ID de objeto se muestran con sus valores actuales. Hay dos objetos importantes:

```
# cfgUserAdminIndex=XX cfgUserAdminUserName=
```

Si el objeto `cfgUserAdminUserName` no tiene valor, el número de índice, que se indica mediante el objeto `cfgUserAdminIndex`, está disponible para usar. Si se muestra un nombre después del signo "=", ese índice lo lleva ese nombre de usuario.

Cuando se activa o desactiva manualmente un usuario con el subcomando racadm `config`, se **debe** especificar el índice con la opción `–i`.

El carácter "#" en los objetos de comando indica que es un objeto de solo lectura. Asimismo, si utiliza el comando `racadm config -f racadm.cfg` para especificar cualquier cantidad de grupos u objetos a escribir, no se puede especificar el índice. Un usuario nuevo se agrega al primer índice disponible. Este comportamiento permite una mayor flexibilidad a la hora de configurar un segundo CMC con los mismos valores que el 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 más información sobre los privilegios de usuario, consulte Types of Users (Tipos de usuarios).
4. Active el usuario.

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.

NOTA: Consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC) a fin de obtener una lista de valores de máscara de bits válidos para privilegios de usuario específicos. El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene activado ningún privilegio.

```
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
```

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 sobre los comandos de RACADM, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)* disponible en **dell.com/support/manuals**.

Desactivación de un usuario del CMC

Al usar RACADM, los usuarios se debe 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 <índice>"" 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 <índice>
   ```

2. Escriba los comandos siguientes con el nombre de usuario y la contraseñas nuevos.

   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <índice> <valor
   de máscara de bits de privilegio del usuario>
   ```

   NOTA: Para obtener una lista de valores de máscara de bits válidos para privilegios de usuario específicos, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)* disponible en **dell.com/support/manuals**. El valor de privilegio predeterminado es 0, lo que indica que el usuario no tiene activado ningún privilegio.

Configuración de usuarios de Active Directory

Si la empresa utiliza el software Microsoft Active Directory, es posible configurar ese software para proporcionar acceso al CMC, lo que permite agregar y controlar los privilegios de usuario del CMC para los usuarios existentes en el servicio de directorio. Esta función requiere una licencia.

NOTA: El uso de Active Directory para reconocer los usuarios del 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.

Es posible configurar la autentificación de usuario a través de Active Directory para iniciar sesión en el CMC. También se puede proporcionar autorización basada en funciones, lo que permite que un administrador configure privilegios específicos para cada usuario.

Mecanismos de autentificación compatibles de Active Directory

Es posible utilizar Active Directory para definir el acceso de usuario al CMC mediante dos métodos:

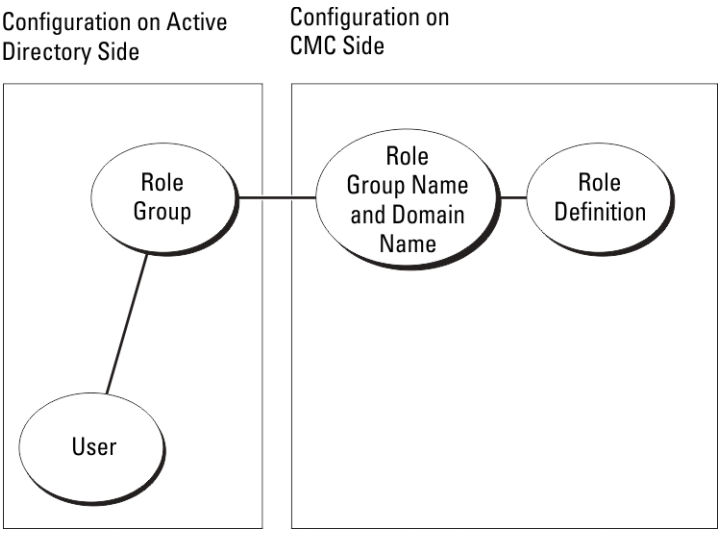
- La solución de *esquema estándar*, que solo utiliza objetos de grupo predeterminados de Active Directory de Microsoft.
- La solución de *esquema extendido*, que tiene objetos de Active Directory personalizados provistos por Dell. Todos los objetos de control de acceso se mantienen en Active Directory. Proporciona una flexibilidad máxima a la hora de configurar el acceso de usuario en distintos CMC con niveles de privilegios variados.

Enlaces relacionados

Descripción general del esquema estándar de Active Directory
Descripción general del esquema extendido de Active Directory

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 el CMC.



En Active Directory, un objeto de grupo estándar se utiliza como grupo de funciones. Un usuario con acceso al 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 tabla siguiente se muestran los privilegios predeterminados del grupo de funciones.

Tabla 19. : Privilegios predeterminados del grupo de funciones

Grupo de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
1	Ninguno	• Usuario con acceso al CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Server Administrator • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A • Administrador de red Fabric B	0x00000fff

Grupo de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
		• Administrador de red Fabric C	
2	Ninguno	• Usuario con acceso al CMC • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Server Administrator • 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 al 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 el complemento **Usuarios y equipos de Active Directory**.
2. Mediante la interfaz web del 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 al 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 **Descripción general del chasis** y haga clic en **Autentificación de usuario** → **Servicios de directorio**. Aparecerá la página **Servicios de directorio**.
2. Seleccione **Microsoft Active Directory (Esquema estándar)**. Los valores que se deben configurar para el esquema estándar se muestran 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 **Configuración del esquema estándar**, haga clic en una opción de **Grupo de funciones**. Aparecerá la página **Configurar grupo de funciones**.
6. Especifique el nombre del grupo, el dominio y los privilegios para el grupo de funciones.
7. Haga clic en **Aplicar** para guardar la configuración del grupo de funciones y haga clic en **Volver a la página de configuración**.
8. Si ha activado la validación de certificados, debe cargar en el CMC el certificado firmado por una autoridad de certificados raíz para el bosque de dominio. En la sección **Administrar certificados**, escriba la ruta de acceso del archivo o busque el archivo de certificado. Haga clic en **Cargar** para cargar el archivo en el CMC.

   NOTA: El valor **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo de certificado que se desea cargar. Debe escribir la ruta de acceso absoluta del archivo, lo que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

   Los certificados SSL para las controladoras de dominio deben estar firmados por el certificado con la firma de la autoridad de certificados raíz. El certificado con la firma de la autoridad de certificados raíz debe estar disponible en la estación de administración que tiene acceso al CMC.
9. Si ha activado el inicio de sesión único (SSO), en la sección **Archivo keytab de Kerberos**, haga clic en **Examinar**, especifique el archivo keytab y haga clic en **Cargar**. Una vez completada la carga, se mostrará un mensaje donde se indicará si la carga se ha realizado correctamente o ha fallado.
10. Haga clic en **Aplicar**. El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.
11. Cierre sesión y luego inicie sesión en el CMC para completar la configuración de Active Directory en el CMC.
12. Seleccione **Chasis** en el árbol del sistema y desplácese hasta la ficha **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 del servidor DNS, desactive la opción **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 <nombre de dominio raíz completo> racadm config -g
   cfgStandardSchema -i <índice> -o cfgSSADRoleGroupName <nombre común de
   grupo de funciones> racadm config -g cfgStandardSchema -i <índice>-o
   cfgSSADRoleGroupDomain <nombre de dominio completo> racadm config -g
   cfgStandardSchema -i <índice> -o cfgSSADRoleGroupPrivilege <número de
   máscara de bits para permisos de usuario específicos> racadm sslcertupload -
   t 0x2 -f <certificado de CA raíz para ADS> racadm sslcertdownload -t 0x1 -f
   <certificado SSL para RAC>
   ```

   NOTA: Para ver los valores de número de la máscara de bits, consulte el capítulo de propiedades de la base de datos en *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

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

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 forman 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 incluir el nombre, el apellido, el número de teléfono y otros datos del usuario.

Para extender la base de datos de Active Directory, es posible agregar *atributos* y *clases* únicos propios para requisitos específicos. Dell ha extendido el esquema para incluir los cambios necesarios y admitir la autorización y la autentificación de la administración remota mediante Active Directory.

Cada *atributo* o *clase* que se agrega a un esquema existente de Active Directory debe definirse con una identificación única. Para mantener las identificaciones únicas en todo el sector, Microsoft mantiene una base de datos de identificadores de objetos de Active Directory (OID) para que cuando las empresas agreguen extensiones al esquema, puedan tener la garantía de que serán únicos y no entrarán en conflicto entre sí. Para extender el esquema en Microsoft Active Directory, Dell recibe OID únicos, extensiones de nombre únicas e identificaciones de atributos con vínculos únicos para los atributos y las clases que se agregan al servicio de directorio.

- Extensión de Dell: `dell`
- OID base de Dell: `1.2.840.113556.1.8000.1280`
- Rango de LinkID del RAC: `12070` a `12079`

Descripción general sobre las extensiones de esquema

Dell ha extendido el esquema para incluir una propiedad *Asociación*, *Dispositivo* y *Privilegio*. La propiedad *Asociación* se utiliza para vincular los usuarios o grupos con un conjunto específico de privilegios para uno o varios dispositivos de RAC. Este modelo proporciona a un administrador la flexibilidad máxima sobre las distintas combinaciones de usuarios, privilegios de RAC y dispositivos de RAC en la red sin demasiada complexidad.

Si existen dos CMC en la red que se desean integrar a Active Directory para fines de autentificación y autorización, es necesario crear al menos un objeto de asociación y un objeto de dispositivo de RAC para cada CMC. Es posible crear varios objetos de asociación y cada objeto de asociación puede ser vinculado a cuantos usuarios, grupos de usuarios u objetos de dispositivo de RAC sea necesario. Los usuarios y objetos de dispositivo de RAC pueden ser miembros de cualquier dominio en la empresa.

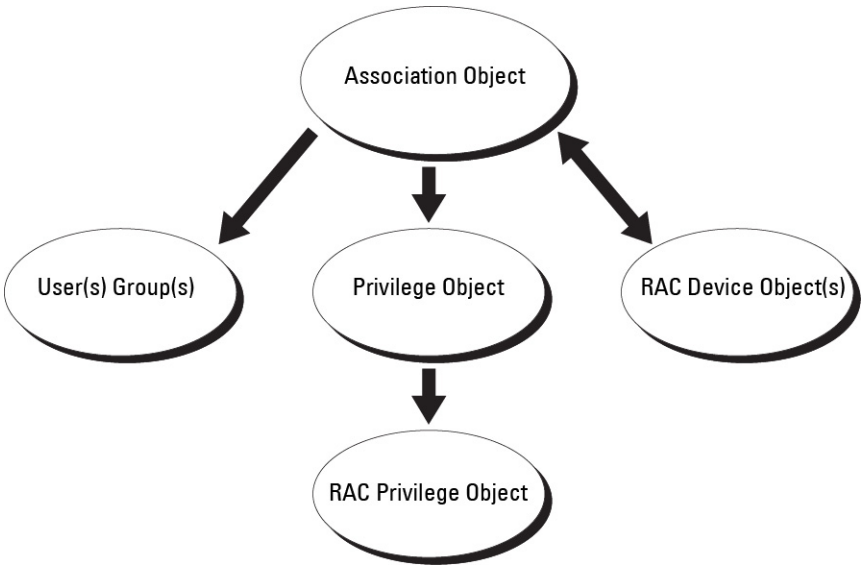
Sin embargo, cada objeto de asociación puede ser vinculado (o puede unir usuarios, grupos de usuarios u objetos de dispositivo de RAC) a un solo objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en los CMC específicos.

El objeto del 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.

Es posible crear el número de objetos de asociación que sea necesario. Sin embargo, se debe crear al menos un objeto de asociación y se debe tener un objeto de dispositivo de RAC para cada RAC (CMC) en la red que se desee integrar con Active Directory.

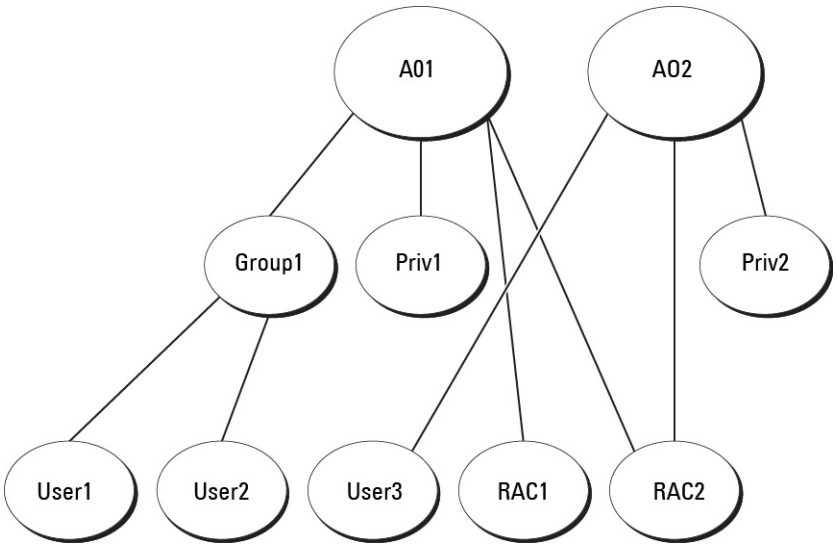


El objeto de asociación permite tener tantos usuarios o grupos como sea necesario, así como objetos de dispositivo de RAC. No obstante, el objeto de asociación solamente incluye un objeto de privilegio por objeto de asociación. El objeto de asociación conecta a los *usuarios* que tienen *privilegios* en los RAC (CMC).

Además, se pueden configurar objetos de Active Directory en un solo dominio o en varios. Por ejemplo, es posible tener dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory existentes (usuario1, usuario2 y usuario3). El usuario puede desear otorgar el privilegio de administrador para ambos CMC a usuario1 y usuario2, y el privilegio de inicio de sesión

en la tarjeta de RAC2 a usuario3. En la siguiente figura se muestra la forma de configurar los objetos de Active Directory en este escenario.

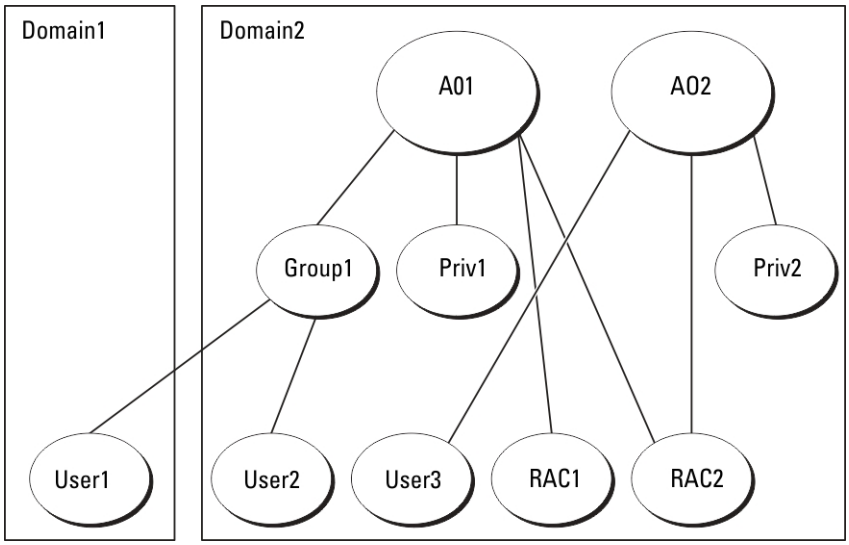
Al agregar grupos universales desde dominios independientes, cree un objeto de asociación con ámbito universal. Los objetos de asociación predeterminados que crea la utilidad Dell Schema Extender son grupos locales de dominios y no funciona con grupos universales de otros dominios.



Para configurar los objetos en un escenario de un solo dominio:

1. Cree dos objetos de asociación.
2. Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representen a los dos CMC.
3. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tenga todos los privilegios (de administrador) y Priv2 tenga el privilegio de inicio de sesión.
4. Agrupe usuario1 y usuario2 en grupo1.
5. Agregue grupo1 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 usuario3 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 los objetos de Active Directory en varios dominios. En este escenario, el usuario dispone de dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory (usuario1, usuario2 y usuario3) existentes. El usuario1 está en el dominio1, y el usuario2 y el usuario 3 están en el dominio2. En este escenario, configure el usuario1 y el usuario2 con privilegios de administrador para ambos CMC, y el usuario3 con privilegios de inicio de sesión para la tarjeta de RAC2.



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 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 user1 y user2 en Grup1. El ámbito de grupo de Grup1 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 al CMC:

1. Amplíe el esquema de Active Directory.
2. Amplíe el complemento Usuarios y equipos de Active Directory.
3. Agregue usuarios del 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.

Enlaces relacionados

Extensión del esquema de Active Directory
Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory
Agregar usuarios y privilegios del CMC a Active Directory
Configuración de Active Directory con esquema extendido mediante la interfaz web del CMC
Configuración de Active Directory con esquema extendido mediante RACADM

Extensión del esquema de Active Directory

Extender el esquema de Active Directory agrega una unidad organizacional de Dell, clases y atributos de esquema y privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender el esquema,

asegúrese de disponer los privilegios de administrador de esquemas en propietario del rol FSMO (operación maestra única flexible del esquema maestro) del bosque de dominios.

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_Advanced \LDIF_Files**
- **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools \Remote_Management_Advanced\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 **Terminar**.

   El esquema se extenderá. Para verificar la extensión del esquema, utilice el complemento de esquema de Active Directory y el MMC para verificar que las clases y los atributos existan. Para obtener más información sobre las clases y los atributos, consulte Classes and Attributes (Clases y atributos). Para obtener detalles sobre el uso del complemento de esquema de Active Directory y el MMC, consulte la documentación de Microsoft.

Clases y atributos

Tabla 20. : 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 21. : Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo de RAC de Dell. RAC debe configurarse como delliDRACDevice en Active Directory. Esta configuración permite que CMC envíe solicitudes de protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
SuperClasses	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 22. : Clase delliDRACAssociationObject

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Descripción	Representa el objeto de asociación de Dell. Este proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
SuperClasses	Group (Grupo)
Atributos	dellProductMembers dellPrivilegeMember

Tabla 23. : Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (derechos de autorización) para el dispositivo CMC.
Tipo de clase	Clase auxiliar
SuperClasses	None (Ninguno)
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tabla 24. : 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	User (Usuario)
Atributos	dellRAC4Privileges

Tabla 25. : 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 26. : Lista de atributos agregados al esquema de Active Directory

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Atributo: `dellPrivilegeMember` **Descripción**: lista de objetos `dellPrivilege` que pertenecen a este atributo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.1 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellProductMembers` **Descripción**: lista de objetos `dellRacDevices` que pertenecen a esta función. Este atributo es el vínculo de avance para el vínculo de retroceso `dellAssociationMembers`. **Identificación de vínculo**: 12070 **OID**: 1.2.840.113556.1.8000.1280.1.1.2.2 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellIsCardConfigAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de configuración de tarjeta en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsLoginUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de inicio de sesión en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.3	VERDADERO

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Atributo: `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.	VERDADERO

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
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)	
Atributo: `dellAssociationMembers` **Descripción**: lista de los objetos dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso para el atributo vinculado dellProductMembers. **Identificación de vínculo**: 12071	FALSO
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)	
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 se instala el software de administración de sistemas mediante el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management), es posible extender el complemento si se selecciona la opción **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 acerca de la instalación del software de administración de sistemas. Para los sistemas operativos Windows de 64 bits, el instalador del complemento se encuentra en: **<Unidad de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn64**.

Para obtener más información acerca del complemento Usuarios y equipos de Active Directory, consulte la documentación de Microsoft.

Agregar usuarios y privilegios del CMC a Active Directory

Mediante el complemento Usuarios y equipos de Active Directory extendido de Dell, es posible agregar usuarios y privilegios del CMC al crear objetos de dispositivo de RAC, de asociación y de privilegio. Para agregar cada objeto, realice los pasos siguientes:

- Cree un objeto de dispositivo de RAC
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Enlaces relacionados

Adición de objetos a un objeto de asociación
Creación de un objeto de dispositivo de RAC
Creación de un objeto de privilegio
Creación de un objeto de asociación

Creación de un objeto de dispositivo de RAC

Para crear un objeto de dispositivo de RAC:

1. En la ventana **Raíz de consola (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. Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del CMC que proporcionó en "Configuring Active Directory With Extended Schema Using CMC Web Interface" (Configuración de Active Directory con esquema extendido con la interfaz web del 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 asociación especifica el tipo de grupo de seguridad para el objeto de asociación. Cuando cree un objeto de asociación, seleccione el ámbito de asociación que se aplica al tipo de objeto que desea agregar. Si selecciona Universal, por ejemplo, los objetos de asociación solamente estarán disponibles cuando Active Directory Domain esté funcionando en modo nativo o en un modo 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

Mediante la ventana **Propiedades de objeto de asociación**, es posible asociar usuarios o grupos de usuarios, objetos de privilegio y dispositivos de RAC o grupos de dispositivos de RAC. Si el sistema ejecuta el modo de Microsoft Windows 2000 o superior, use grupos universales para expandir dominios con el usuario o los 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.

Enlaces relacionados

Adición de usuarios o grupos de usuarios
Adición de privilegios

Forma de agregar dispositivos de RAC o grupos de dispositivos de RAC

Adición de usuarios o grupos de usuarios

Para agregar usuarios o grupos de usuarios:

1. Haga clic con el botón derecho del mouse en **Objeto de asociación** y seleccione **Propiedades**.
2. Seleccione la ficha **Usuarios** y haga clic en **Agregar**.
3. Introduzca el nombre del grupo de usuarios o del usuario y haga clic en **Aceptar**.

Adición de privilegios

Para agregar privilegios:

1. Seleccione la ficha **Objetos de privilegios** y haga clic en **Agregar**.
2. Introduzca el nombre del objeto de privilegio y haga clic en **Aceptar**.

   Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios al autentificar un dispositivo 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 **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: Es posible especificar una lista de servidores de controladora de dominio o de catálogo global separados por comas. El CMC 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` (Ruta de acceso del archivo) muestra la ruta de acceso relativa del archivo de certificado que se desea cargar. Debe escribir la ruta de acceso absoluta del archivo, lo que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

   Los certificados SSL para las controladoras de dominio deben estar firmados por el certificado con la firma de la autoridad de certificados raíz. El certificado con la firma de la autoridad de certificados raíz debe estar disponible en la estación de administración que tiene acceso al CMC.

   PRECAUCIÓN: La validación de certificados SSL se requiere de forma predeterminada. 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 **Apply (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 **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 <nombre de dominio completo de CMC> racadm config -g
cfgActiveDirectory -o cfgADRootDomain <nombre de dominio raíz completo>
racadm config -g cfgActiveDirectory -o cfgADRacName <nombre común de CMC>
racadm sslcertupload -t 0x2 -f <certificado de CA raíz para ADS> -r racadm
sslcertdownload -t 0x1 -f <certificado SSL para CMC>
```

   NOTA: Este comando se puede usar solamente a través de un RACADM remoto. Para obtener más información sobre el RACADM remoto, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

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 **Especificar servidor**, el nombre de host en el 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 **Especificar servidor**, es posible especificar un servidor LDAP y un catálogo global con las direcciones IP o los nombres de dominio completos (FQDN) de los servidores. Los nombres FQDN consisten en los nombres de host y de dominio de los servidores.

Para especificar un servidor de LDAP, escriba:

```
racadm config -g cfgActiveDirectory -o cfgADDomainController <dirección IP
de la controladora de dominio AD>
```

Para especificar un servidor de catálogo global, escriba:

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <dirección IP de
catálogo global AD>
```

NOTA: Si la dirección IP se define con el valor 0.0.0.0, el CMC no puede buscar un servidor.

NOTA: Es posible especificar una lista de servidores de LDAP o de catálogo global separados por comas. El CMC 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 <dirección IP de DNS
     principal> racadm config -g cfgLanNetworking -o cfgDNSServer2
     <dirección IP de DNS secundario>
     ```

De esta forma, se completa la configuración de la función de esquema extendido.

Configuración de los usuarios LDAP genéricos

El CMC proporciona una solución genérica para admitir la autentificación basada en el protocolo ligero de acceso a directorios (LDAP). Esta función no requiere ninguna extensión de esquema en los servicios de directorio.

Ahora un administrador del CMC puede integrar los inicios de sesión de los usuarios del servidor LDAP con el CMC. Esta integración requiere una configuración en el servidor LDAP y en el CMC. En el servidor LDAP, se utiliza un objeto de grupo estándar como un grupo de funciones. Un usuario con acceso al CMC se convierte en miembro del grupo de funciones. Los privilegios se continúan almacenando en el CMC para la autorización, de forma similar a la configuración de esquema estándar compatible con Active Directory.

Para activar el usuario LDAP de modo que tenga acceso a una tarjeta específica del CMC, el nombre del grupo de funciones y su nombre de dominio se deben configurar en la tarjeta específica del CMC. Es posible configurar cinco

grupos de funciones como máximo 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, el usuario 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.

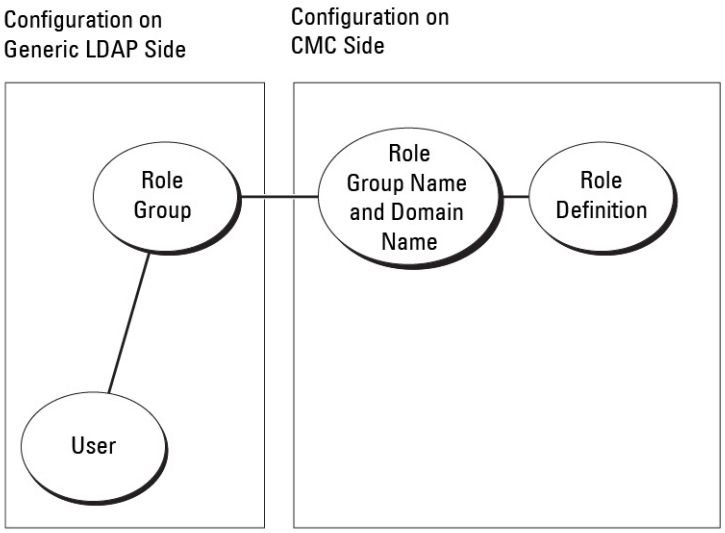


Ilustración 2. Configuración de CMC con LDAP genérico

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. De forma opcional, establezca un enlace con el servicio de directorio. El enlace predeterminado es anónimo.
2. Busque el usuario en función de su inicio de sesión 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. Buscar en cada grupo configurado el nombre de dominio del usuario en 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 **Descripción general del chasis** y haga clic en **Autentificación de usuario** → **Servicios de directorio**.
2. Seleccione **LDAP** genérico.

   Los valores que se deben configurar para el esquema estándar se mostrarán en la misma página.
3. Especifique lo siguiente:

   NOTA: Para obtener información acerca de los distintos campos, consulte *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*> indica el nombre del servicio que se debe utilizar en la consulta.

       Por ejemplo:

       `_ldap._tcp.dell.com`

       donde `ldap` es el nombre del servicio y `dell.com` es el dominio de búsqueda.
4. Haga clic en **Aplicar** para guardar la configuración.

   NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.
5. En la sección **Configuración de grupos**, haga clic en un **Grupo de funciones**. Aparecerá la página **Configurar grupo de funciones 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 **Apply (Aplicar)**.

   Se habrá configurado el servicio de directorio LDAP.

Configuración del servicio de directorio LDAP genérico mediante RACADM

Para configurar el servicio de directorio LDAP, utilice los objetos en los grupos RACADM `cfgLdap` y `cfgLdapRoleGroup`.

Existen muchas opciones para configurar los inicios de sesión de LDAP. En la mayoría de los casos, algunas opciones pueden utilizarse con su configuración predeterminada.

NOTA: Se recomienda especialmente utilizar el comando racadm `testfeature -f LDAP` para probar la configuración inicial de LDAP. Esta función admite IPv4 e IPv6.

Los cambios de propiedades necesarios incluyen la activación de inicios de sesión de LDAP, la definición de un nombre de dominio completo o una dirección IP para el servidor y la configuración del DN de base del servidor LDAP.

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`
- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc= company,dc=com`

El CMC puede configurarse para realizar una consulta opcional en el servidor DNS para solicitar registros de SRV. Si la propiedad `cfgLDAPSRVLookupEnable` está activada, la propiedad `cfgLDAPServer` no se toma en cuenta. La siguiente consulta se utiliza para buscar registros de SRV en el DNS:

`_ldap._tcp.domainname.com`

En esta consulta, `ldap` es la propiedad `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` se configura para ser **domainname.com**.

Para obtener más información sobre los objetos RACADM, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)* 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 el 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 a las aplicaciones subsiguientes como Exchange. Para el inicio de sesión único, el CMC utiliza las credenciales del sistema cliente que el sistema operativo almacena en caché después de que el usuario inicia sesión mediante una cuenta de Active Directory válida.

La autentificación de dos factores proporciona un mayor nivel de seguridad, ya que requiere que los usuarios dispongan de una contraseña o PIN y una tarjeta física con una clave privada o un certificado digital. Kerberos usa este mecanismo de autentificación de dos factores, con el que los sistemas pueden probar su autenticidad.

NOTA: Cuando se selecciona un método de inicio de sesión, no se determinan los atributos de política relacionados con otras interfaces de inicio de sesión, por ejemplo, SSH. Se deben establecer otros atributos de política para las demás interfaces de inicio de sesión. Para desactivar todas las demás interfaces de inicio de sesión, vaya a la página **Servicios** y desactive todas las interfaces de inicio de sesión (o algunas de ellas).

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.

Enlaces relacionados

Requisitos del sistema

Prerrequisitos para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente

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

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 el 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 el 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 el CMC).

Enlaces relacionados

Configuración del esquema estándar de Active Directory
Configuración del esquema extendido de Active Directory
Configuración del explorador para el inicio de sesión único
Generación del archivo Keytab de Kerberos
Configuración de un explorador para el inicio de sesión mediante tarjeta inteligente

Generación del archivo Keytab de Kerberos

Para admitir la autentificación de inicio de sesión único y de inicio de sesión mediante tarjeta inteligente, el CMC admite la red Kerberos de Windows. La herramienta ktpass (disponible en Microsoft como parte de los CD/DVD de instalación de servidores) se utiliza para crear enlaces de nombre principal de servicio (SPN) a una cuenta de usuario y exportar la

información de confianza a un archivo keytab de Kerberos de estilo MIT. Para obtener más información sobre la utilidad ktpass, consulte el sitio web de Microsoft.

Antes de generar un archivo keytab, debe crear una cuenta de usuario de Active Directory para utilizar con la opción **-mapuser** del comando ktpass. Debe usar el mismo nombre que el nombre DNS del CMC al que desea cargar el archivo keytab generado.

Para generar un archivo keytab mediante la herramienta ktpass:

1. Ejecute la utilidad *ktpass* en la controladora de dominio (servidor de Active Directory) donde desee asignar el CMC a una cuenta de usuario en Active Directory.
2. Utilice el comando `ktpass` siguiente para crear el archivo keytab de Kerberos:

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

   NOTA: Según los requisitos de RFC, el elemento `nombredecmc.nombre_de_dominio.com` se debe escribir en minúscula y `@REALM_NAME` en mayúscula. Además, 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 el CMC utiliza el inicio de sesión único con la autentificación de Kerberos.

Internet Explorer

Para configurar Internet Explorer para inicio de sesión único:

1. En Internet Explorer, seleccione **Herramientas** → **Opciones de Internet**.
2. En la ficha **Seguridad**, en **Seleccione una zona para ver o cambiar la configuración de seguridad**, seleccione **Intranet local**.
3. Haga clic en **Sitios**.

   Se muestra el cuadro de diálogo **Intranet local**.
4. Haga clic en **Avanzado**.

   Se muestra el cuadro de diálogo **Configuración avanzada de Intranet local**.
5. En el campo **Agregar este sitio a la zona**, escriba el nombre del CMC y el dominio al cual pertenece y haga clic en **Agregar**.

   NOTA: Se puede utilizar un comodín (*) para especificar todos los dispositivos o usuarios de ese dominio.

Mozilla Firefox

1. En Firefox, escriba **about:config** en la barra de direcciones.

   NOTA: Si el explorador muestra la advertencia **Esto puede anular su garantía**, haga clic en **Seré cuidadoso, lo prometo**.

2. En el cuadro de texto **Filtro**, escriba **negotiate**.

   El explorador muestra una lista de nombres preferidos limitada a aquéllos que contienen la palabra "negotiate".

3. En la lista, haga doble clic en **network.negotiate-auth.trusted-uris**.

4. En el cuadro de diálogo **Ingresar valor de la cadena**, escriba el nombre de dominio del CMC y haga clic en **Aceptar**.

Configuración de un explorador para el inicio de sesión mediante tarjeta inteligente

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.

Enlaces relacionados

Prerrequisitos para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente

Cómo cargar el archivo keytab

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 <usuario>@<dominio>
   ```

   donde `<usuario>` es una cuenta de usuario de Active Directory válida.

Una ejecución satisfactoria de este comando indica que el CMC puede adquirir las credenciales Kerberos y obtener acceso a la cuenta de Active Directory del usuario. Si el comando no se ejecuta satisfactoriamente, resuelva el error y vuelva a ejecutar el comando. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC) en **dell.com/support/manuals**.

Cómo cargar el archivo keytab

El archivo keytab de Kerberos sirve como credencial de nombre de usuario y contraseña del 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.

Es posible cargar un archivo keytab de Kerberos generado en el servidor de Active Directory asociado. Al ejecutar la utilidad **ktpass.exe**, se puede generar el archivo keytab de Kerberos desde un servidor de Active Directory. Este archivo keytab establece una relación de confianza entre el servidor de Active Directory Server y el CMC.

Para cargar el archivo keytab:

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 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 -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Además de los pasos que se realizan durante la configuración de Active Directory, utilice los siguientes objetos para activar el inicio de sesión mediante tarjeta inteligente:

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

Configuración del CMC para el uso de consolas de línea de comandos

En esta sección se proporciona información acerca de las funciones de la consola de línea de comandos (o la consola de conexión serie/Telnet/Secure Shell) del CMC y se explica la forma de configurar el sistema para poder ejecutar acciones de administración de sistemas a través de la consola. Para obtener información sobre el uso de los comandos RACADM en el CMC a través de la consola de línea de comandos, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

Enlaces relacionados

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

Funciones de la consola de línea de comandos del CMC

El 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 se conecta a la consola serie de servidores y a los módulos de E/S; también disponible como `racadm connect`.
- Historial y edición de línea de comandos.
- Control del tiempo de espera de las sesiones en todas las interfaces de consola.

Comandos para la línea de comandos del CMC

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

Tabla 27. : Comandos para la línea de comandos del CMC

Comando	Descripción
`racadm`	Los comandos RACADM comienzan con la palabra clave `racadm` seguida de un subcomando. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.
`connect`	Establece una conexión a la consola serie de un servidor o módulo de E/S. Para obtener más información, consulte Connecting to Servers or I/O Modules Using Connect Command (Conexión a servidores o módulos de E/S mediante el comando connect). **NOTA:** También se puede usar el comando racadm `connect`.

Comando	Descripción
`exit`, `logout` y `quit`	Todos estos comandos ejecutan la misma acción. Terminan la sesión actual y regresan a la pantalla de inicio de sesión.

Uso de una consola Telnet con el CMC

Es posible mantener hasta cuatro sesiones Telnet con el 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 del CMC. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión en el que la tecla Entrar no responde y no aparece la petición de contraseña.

Para solucionar este problema, descargue el hotfix 824810 de **support.microsoft.com**. Además, puede consultar el artículo 824810 de Microsoft Knowledge Base para obtener más información.

Uso de SSH con el CMC

SSH es una sesión de línea de comandos que incluye las mismas funciones que una sesión Telnet, pero con negociación de sesiones y cifrado para mejorar la seguridad. El CMC admite la versión 2 de SSH con autentificación de contraseña. SSH está activado en el CMC de manera predeterminada.

NOTA: El CMC no admite la versión 1 de SSH.

Cuando se presenta un error durante el inicio de sesión en CMC, el cliente SSH envía un mensaje de error. El texto del mensaje depende del cliente y no es controlado por el CMC. Revise los mensajes de RACLog para determinar la causa de la falla.

NOTA: `OpenSSH` se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. También se puede ejecutar `OpenSSH` con **Putty.exe**. Si se ejecuta `OpenSSH` en el símbolo del sistema de Windows, no se obtendrá una funcionalidad completa (es decir, algunas teclas no responderán y no se mostrarán gráficos). Para sistemas que ejecutan Linux, ejecute los servicios cliente de SSH para conectarse al CMC con cualquier shell.

Se admiten cuatro sesiones simultáneas de SSH en un momento dado. La propiedad `cfgSsnMgtSshIdleTimeout` controla el tiempo de espera de la sesión. Para obtener más información, consulte el capítulo sobre propiedades de la base de datos de *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*, la página **Administración de servicios** de la interfaz web, o consulte Configuring Services (Configuración de servicios).

El CMC también admite la autentificación de clave pública (PKA) sobre SSH. Este método de autentificación mejora la automatización de secuencias de comandos de SSH gracias a que evita la necesidad de incorporar o solicitar la identificación o la contraseña del usuario. Para obtener más información, consulte Configure Public Key Authentication over SSH (Configuración de la autentificación de clave pública en SSH).

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

Para configurar SSH, consulte Configuring Services (Configuración de servicios).

Enlaces relacionados

Configuración de servicios

Esquemas de criptografía SSH compatibles

Para comunicarse con el CMC mediante el protocolo SSH, se admiten varios esquemas de criptografía que se enumeran en la tabla siguiente.

Tabla 28. : 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

Es posible 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 una clave. El nombre de usuario service es una cuenta de usuario especial que se puede utilizar para acceder al 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 el 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. El CMC no realiza comprobaciones para verificar que las claves anteriores se hayan eliminado antes de agregar una nueva. Tan pronto como se agrega una clave nueva, esa clave entra en vigor automáticamente siempre y cuando la interfaz de SSH esté activada.

Cuando utilice la sección de comentario de la clave pública, recuerde que el CMC solo utiliza los primeros 16 caracteres. El CMC utiliza el comentario de la clave pública para distinguir a los usuarios de SSH cuando utilizan el comando `getssninfo` de RACADM, 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 *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

Enlaces relacionados

Generación de claves públicas para sistemas que ejecutan Windows
Generación de claves públicas para sistemas que ejecutan Linux
Notas de la sintaxis de RACADM para CMC
Visualización de claves públicas
Adición de claves públicas
Eliminación de claves públicas

Generación de claves públicas para sistemas que ejecutan Windows

Antes de agregar una cuenta, se requiere una clave pública del sistema que obtendrá acceso al CMC mediante SSH. Hay dos maneras de generar el par de claves pública-privada: mediante la aplicación Generador de claves PuTTY para clientes que ejecutan Windows o la CLI ssh-keygen para clientes que ejecutan Linux.

En esta sección se describen instrucciones sencillas para generar un par de claves pública-privada en ambas aplicaciones. Para ver usos adicionales o avanzados de estas herramientas, consulte la 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 o SSH-2 DSA para el tipo de clave que generará (SSH-1 no es compatible).
2. Especifique la cantidad de bits para la clave. El número debe estar entre 768 y 4096.

   NOTA: Es posible que el CMC no muestre un mensaje si se agregan claves menores de 768 o mayores de 4096, pero estas claves fallan al intentar iniciar sesión.
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 se puede especificar una frase de contraseña para proteger la clave. Asegúrese de guardar la clave privada.
4. Hay dos opciones para utilizar la clave pública:
   - Guardar la clave pública en un archivo para cargarlo más tarde.
   - Copiar y pegar el texto de la ventana **Clave pública para pegar** al agregar la cuenta mediante la opción de texto.

Generación de claves públicas para sistemas que ejecutan Linux

La aplicación ssh-keygen para los clientes Linux es una herramienta de línea de comandos sin interfaz gráfica de usuario. Abra una ventana de terminal y, en el indicador de shell, escriba:

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

donde:

La opción `-t` debe ser dsa o rsa.

La opción `-b` especifica el tamaño de cifrado de bits entre 768 y 4096.

La opción `-c` permite modificar el comentario de clave pública y es opcional.

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

Notas de la sintaxis de RACADM para CMC

Cuando utilice el comando `racadm sshpkauth`, asegúrese de cumplir estos requisitos:

- Para la opción `–i`, el parámetro debe ser `svcacct`. Todos los demás parámetros para `–i` fallan en el CMC. `svcacct` es una cuenta especial para la autentificación de clave pública sobre SSH en el CMC.
- Para iniciar sesión en el 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` por un número de 1 a 6. Por ejemplo, para ver la clave 2, escriba:

```
racadm sshpkauth –i svcacct –k 2 –v
```

Adición de claves públicas

Para agregar una clave pública al CMC mediante la opción de carga de archivo `–f`, escriba:

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –f <archivo de clave pública>
```

NOTA: Es posible usar solo la opción de carga de archivo con RACADM remoto. Para obtener más información, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

Para agregar una clave pública mediante la opción de carga de texto, escriba:

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –t "<archivo de clave pública>"
```

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 de puerto 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. Para configurar otras versiones de Minicom, consulte la información en la sección Required Minicom Settings (Valores de Minicom requeridos).

Configuración de Minicom versión 2.0

NOTA: Para obtener mejores resultados, defina la propiedad **cfgSerialConsoleColumns** de manera que coincida con la cantidad de columnas. Tenga en cuenta que la petición ocupa dos caracteres. Por ejemplo, para una ventana de terminal con 80 columnas, la propiedad es:

```
racadm config –g cfgSerial –o cfgSerialConsoleColumns 80.
```

1. Si no tiene el archivo de configuración de Minicom, vaya al siguiente paso. Si lo tiene, escriba `minicom<Minicom config file name>` y avance al paso 12.
2. En la petición de comandos de Linux, escriba `minicom -s`.
3. Seleccione **Configuración del puerto serie** y presione <Intro>.
4. Presione <a> y seleccione el dispositivo de serie correspondiente (por ejemplo, `/dev/ttyS0`).
5. Presione <e> y defina la opción **Bps/Par/Bits** con el valor **115200 8N1**.
6. Presione <f> y defina la opción **Control de flujo de hardware** en el valor **Sí** y luego defina la opción **Control de flujo de software** en el valor **No**. Para salir del menú **Configuración del puerto serie**, presione <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 la petición de shell de comandos, 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 esta aparezca, la conexión se habrá completado con éxito. Desde ese momento, podrá iniciar sesión y obtener acceso a la interfaz de línea de comandos de CMC.

Valores de Minicom necesarios

Consulte la siguiente tabla para configurar cualquier versión de Minicom.

Tabla 29. : Valores 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 E/S 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 *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)* 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, el CMC admite el comando connect para establecer una conexión serie con el servidor o los módulos de E/S. La consola serie del servidor contiene las pantallas de inicio y configuración del BIOS y la consola serie del sistema operativo. Para los módulos de E/S, la consola serie del conmutador está disponible.

PRECAUCIÓN: Cuando se ejecuta desde la consola serie del CMC, la opción `connect -b` permanece conectada hasta que se restablece el CMC. Esta conexión es un riesgo potencial de seguridad.

NOTA: El comando `connect` ofrece la opción `–b` (binario). La opción `–b` transmite datos binarios sin procesar y no utiliza `cfgSerialConsoleQuitKey`. Además, al establecer conexión con un servidor por medio de la consola serie del 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 la redirección de consola, el comando `connect` muestra una consola vacía. En tal caso, para regresar a la consola del CMC, escriba la secuencia de escape. La secuencia de escape predeterminada de la consola es <Ctrl><\>.

Existe un máximo de seis módulos de E/S en el sistema administrado. Para conectar un módulo de E/S:

```
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 30. : 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 del servidor administrado, use 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`Al establecer conexión con un servidor mediante la opción `–b`, se asume la existencia de una comunicación binaria y el carácter de escape se desactiva. Si el iDRAC no se encuentra disponible, aparecerá el mensaje de error `No route to host` (No hay ruta al host).

El comando `connect server-n` permite que el usuario obtenga acceso al puerto serie del servidor. Tras establecerse la conexión, el usuario podrá ver la redirección de consola del servidor a través del puerto serie del 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 establecer en 80x25. De modo 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.

Enlaces relacionados

Configuración del BIOS del servidor administrado para la redirección de consola serie
Configuración de Windows para la redirección de consola en serie
Configuración de Linux para la redirección de la consola en serie del servidor durante el inicio
Configuración de Linux para la redirección de consola serie del servidor después del inicio

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

Es necesario conectarse al servidor administrado por medio del iKVM (consulte Managing Servers With iKVM [Administración de servidores con iKVM]) o establecer una sesión de la consola remota desde la interfaz web del iDRAC7 (consulte *iDRAC7 User's Guide [Guía del usuario del iDRAC7]* 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, se 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 **Comunicación serie** y presione <Intro>. En el cuadro de diálogo emergente, la lista de comunicación serie muestra las siguientes opciones:
   - Off (Desactivado)
   - 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 **Redirección después de inicio** (el valor predeterminado es **Desactivado**). Esta opción permite la redirección de consola del BIOS en inicios posteriores.
6. Guarde los cambios y salga.
   El servidor administrado se reinicia.

Configuración de Windows para la redirección de consola en serie

No es necesario configurar los servidores que ejecutan versiones de Microsoft Windows Server, a partir de Windows Server 2003. Windows recibirá información del BIOS y activará la consola de administración especial (SAC) COM1.

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

Los pasos siguientes se aplican a Linux GRand Unified Bootloader (GRUB). Se deben realizar cambios similares si se utiliza un cargador de inicio diferente.

NOTA: 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:
   ```
   consola de núcleo=ttyS1,57600
   ```
3. Si el archivo **/etc/grub.conf** contiene una directiva `splashimage`, inserte un carácter de comentario al inicio de la línea para anularla.

   El siguiente ejemplo ilustra los cambios descritos en este procedimiento.

   ```
   # grub.conf generated by anaconda # # Note that you do not have to rerun
   grub after making changes # to this file # NOTICE: You do not have a /boot
   partition. This means that # all kernel and initrd paths are relative to /,
   e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root= /dev/sda1 #
   initrd /boot/initrd-version.img # #boot=/dev/sda default=0 timeout=10
   #splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600 terminal --timeout=10
   serial title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /
   boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0
   console= ttyS1,57600 initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat
   Linux Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/
   vmlinuz-2.4.9-e.3 ro root=/dev/sda1 initrd /boot/initrd-2.4.9-e.3.img
   ```

   Cuando edite el archivo **/etc/grub.conf**, siga estas pautas:

   - Desactive la interfaz gráfica de GRUB y utilice la interfaz basada en texto. De lo contrario, la pantalla GRUB no se mostrará en la redirección de consola. Para desactivar la interfaz gráfica, inserte un carácter de comentario en la línea que comienza con `splashimage`.
   - Para abrir varias opciones de GRUB a fin de iniciar sesiones de consola por medio de la conexión en serie, agregue la siguiente línea a todas las opciones:

     ```
     consola=ttyS1,57600
     ```

     El ejemplo muestra el elemento `consola=ttyS1,57600` agregado sólo a 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.

Enlaces relacionados

Acerca de FlexAddress
Acerca de FlexAddress Plus
Comparación entre FlexAddress y FlexAddress Plus

Acerca de FlexAddress

La función FlexAddress es una actualización opcional que permite a los módulos del servidor reemplazar las identificaciones de red Nombre mundial y Control de acceso medios (WWN/MAC) asignadas de fábrica con identificaciones WWN/MAC proporcionadas por el chasis.

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

FlexAddress permite que el CMC asigne identificaciones de WWN/MAC a una ranura determinada y sobrescriba las identificaciones de fábrica. Si se sustituye el módulo de servidor, la identificación de WWN/MAC basada en la ranura no cambia. Gracias a esta función, ya no es necesario volver a configurar las herramientas de administración de red Ethernet y los recursos SAN para un nuevo módulo de servidor.

Además, las identificaciones solo se *sobrescriben* cuando se inserta un módulo de servidor en un chasis compatible con FlexAddress; no se realizan cambios permanentes en el módulo de servidor. Si se mueve un módulo de servidor a un chasis que no admite FlexAddress, se utilizan las identificaciones de WWN/MAC asignadas de fábrica.

La tarjeta de función FlexAddress contiene un rango de direcciones MAC. Antes de instalar FlexAddress, puede determinar este rango insertando la tarjeta SD en un lector de tarjetas de memoria USB y visualizando el archivo **pwwn_mac.xml**. Este archivo XML de texto contiene una etiqueta XML *mac_start* que es la primera dirección MAC hexadecimal de inicio que se utiliza para este rango exclusivo de direcciones MAC. La etiqueta *mac_count* es la cantidad total de direcciones MAC que asigna la tarjeta SD. El rango MAC total asignado puede determinarse en función de:

```
<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 + 0xCF = (ending_mac)00188BFFDDC9
```

NOTA: Bloquee la tarjeta SD antes de insertarla en el lector de tarjetas de memoria USB para evitar modificar accidentalmente el contenido. *Debe desbloquear* la tarjeta SD antes de insertarla en el CMC.

Acerca de FlexAddress Plus

FlexAddress Plus es una nueva función que se agrega a la versión 2.0 de la tarjeta de función. Se trata de una actualización de la tarjeta de función FlexAddress versión 1.0. La función FlexAddressPlus contiene más direcciones MAC que FlexAddress. Ambas funciones permiten que el chasis asigne direcciones WWN/MAC (Nombre mundial/ Control de acceso de medios) a dispositivos Fibre Channel y Ethernet. Las direcciones WWN/MAC asignadas por el chasis son únicas 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.

	Red Fabric A	Red Fabric B	Red Fabric C	Administración del iDRAC	Total de direcciones MAC
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

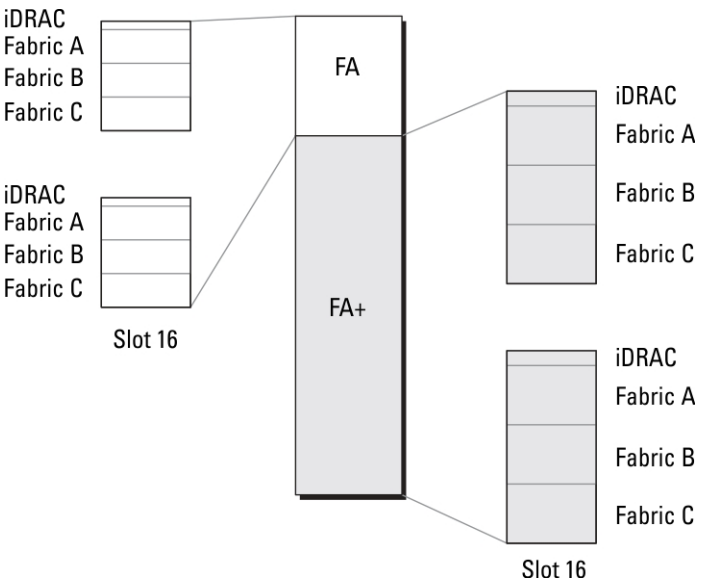


Ilustración 3. Funciones de FlexAddress (FA) y FlexAddress Plus (FA+)

Activación de FlexAddress

FlexAddress se presenta en una tarjeta Secure Digital (SD) que se debe insertar en el CMC para activar la función. Es posible que se requiera de varias actualizaciones de software para activar la función FlexAddress; si no se 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 del CMC. Es necesario aplicar dichas actualizaciones antes de activar FlexAddress. De lo contrario, es posible que FlexAddress no funcione del modo esperado.

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 contenida en la tarjeta SD está cifrada y no es posible duplicarla o alterarla de ninguna forma porque podría desactivar las funciones del sistema y ocasionar que el sistema deje de funcionar.

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 al reiniciar el CMC con la tarjeta de función SD instalada. Esta activación hace que la función se enlace al chasis actual. Si tiene la tarjeta SD instalada en el CMC redundante, la activación de la función FlexAddress no se produce hasta tanto se vuelva activo el CMC redundante. 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 información sobre cómo volver activo un CMC redundante.

Cuando se reinicia el CMC, verifique el proceso de activación. Para obtener más información, consulte Verifying FlexAddress Activation (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 etiquetada con el texto FlexAddress solamente contiene FlexAddress y la tarjeta etiquetada con el texto FlexAddress Plus contiene FlexAddress y FlexAddress Plus. Inserte la tarjeta en el CMC para activar la función.

Es posible que algunos servidores, como PowerEdge M710HD, requieran más direcciones MAC de las que FA puede proporcionar al CMC, según como estén configurados. Para estos servidores, la actualización a FA+ permite la optimización completa de la configuración de WWN/MAC. Póngase en contacto con Dell para obtener asistencia para la función FlexAddress Plus.

Para activar la función FlexAddress Plus, se requiere realizar las siguientes actualizaciones de software: BIOS del servidor, iDRAC del servidor y firmware del CMC. Si no se aplican estas actualizaciones, solo la función FlexAddress estará disponible. Para obtener información sobre las versiones mínimas requeridas de estos componentes, consulte *Léame* 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 31. Mensajes de estado que muestra el comando featurecard -s

Mensaje de estado	Acciones
No se insertó ninguna tarjeta de función.	Revise el CMC para verificar que la tarjeta SD se haya insertado correctamente. En una configuración redundante del CMC, asegúrese de que el CMC con la tarjeta de función SD instalada sea el CMC activo y no el 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.

Mensaje de estado	Acciones
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 llevar a otro chasis o se puede reactivar en el chasis actual. Para reactivarla en el chasis actual, introduzca `racadm racreset` hasta que el módulo del 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:

```
Función = Fecha de FlexAddress activada = 8 de abril de 2008 - 10:39:40 Función
instalada de SN de la tarjeta SD = 01122334455
```

Si no hay funciones activas en el chasis, el comando mostrará un mensaje:

```
racadm feature -s No features active on the chassis (racadm feature -s No hay
funciones activas en el chasis)
```

Es posible que Dell Feature Cards pueda contener más de una función. Una vez activada cualquiera de las funciones que incluye Dell Feature Card en un chasis, todas las demás funciones que se puedan incluir en Dell Feature Card no se podrán activar en un chasis diferente. En este 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
(ERROR: Una o más funciones de la tarjeta SD se encuentran activas en otro
chasis)
```

Para obtener más información sobre los comandos **feature** y **featurecard**, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*.

Desactivación de FlexAddress

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

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
(ERROR: No se puede desactivar la función porque el chasis está encendido)
```

Para obtener más información sobre el comando, consulte la sección del comando **feature** de *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*.

Visualización de la información de FlexAddress

Es posible ver información del estado del chasis completo o de un servidor individual. La información que se muestra incluye:

- Configuración de la red Fabric.
- Si FlexAddress está activo o no activo.
- Número y nombre de la ranura.
- Direcciones asignadas por el chasis y por el servidor.
- Direcciones en uso.

Enlaces relacionados

Visualización de la información de FlexAddress del chasis
Visualización de la información de FlexAddress para todos los servidores
Visualización de la información de FlexAddress para servidores individuales

Visualización de la información de FlexAddress del chasis

Es posible mostrar la información de estado de FlexAddress de todo el chasis. La información de estado incluye si la función está activa y una descripción general del estado de FlexAddress de cada servidor.

Para ver el estado de FlexAddress del chasis mediante la interfaz web del CMC, haga clic en **Descripción general del chasis** → **Configuración** → **General**.

Aparecerá la página **Configuración general del chasis**.

FlexAddress tiene un valor **Activo** o **No activo**. El valor **Activo** indica que la función está instalada en el chasis, mientras que **No activo** indica que la función no está instalada y no está en uso en el chasis.

Utilice el siguiente comando de RACADM para mostrar el estado de FlexAddress de todo el chasis:

```
racadm getflexaddr
```

Para mostrar el estado de FlexAddress para una ranura particular:

```
racadm getflexaddr [-i <slot#>]
```

donde *<n.º de ranura>* es un valor entre 1 y 16.

Para obtener información adicional sobre el comando **getflexaddr**, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)* en **dell.com/support/manuals**.

Visualización de la información de FlexAddress para todos los servidores

Para ver el estado de FlexAddress para todos los servidores mediante la interfaz web del CMC, en el árbol del sistema, vaya a **Descripción general del servidor** → **Propiedades** → **WWN/MAC**.

Aparecerá la página **Resumen de WWN/MAC**, que muestra la siguiente información para todas las ranuras en el chasis.

Configuración de la red Fabric	Red Fabric A, Red Fabric B y Red Fabric C muestran los tipos de red Fabric de entrada/salida instalados. iDRAC muestra la dirección MAC de administración del servidor. **NOTA:** Si la red Fabric A está activada, las ranuras desocupadas mostrarán las direcciones MAC asignadas por el chasis para la red Fabric A y las direcciones MAC o WWN para las redes Fabric B y C si están siendo utilizadas por ranuras ocupadas.
Direcciones WWN/MAC	Muestra la configuración de FlexAddress para cada ranura del chasis. La información que se muestra incluye: • Número y ubicación de la ranura. • Si FlexAddress está activo o no activo. • Tipo de red Fabric. • Direcciones WWN/MAC en uso asignadas por el servidor y por el chasis. Una marca verde indica el tipo de dirección activada, ya sea asignada por el servidor o por el chasis. **NOTA:** La controladora de administración del iDRAC no es una red Fabric pero el FlexAddress de este se trata como si lo fuera.

NOTA: FlexAddress no es compatible con EqualLogic PS-M4110 Blade Array.

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

Visualización de la información de FlexAddress para servidores individuales

Para ver la información de FlexAddress para un servidor en particular 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** que proporciona la configuración de WWN y las direcciones MAC para el servidor seleccionado. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.

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.

Debe adquirir e instalar la actualización de FlexAddress para configurar la función FlexAddress. De lo contrario, aparecerá el siguiente texto en la interfaz web:

```
Función opcional no instalada. Consulte Dell Chassis Management Controller
Users Guide (Guía del usuario de Dell Chassis Management Controller) para
obtener información sobre la función de administración de direcciones WWN y MAC
basadas en el chasis. Para adquirir la función, visite el sitio de Dell
www.dell.com.
```

Si adquiere FlexAddress junto con el chasis, la función se instala y se activa al encender el sistema. Si adquiere FlexAddress por separado, deberá 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]) en **dell.com/support/manuals.**

El servidor debe estar apagado para iniciar la configuración. Puede activar o desactivar FlexAddress en cada red Fabric. Otra opción es activar o desactivar la función en cada ranura. Después de activarla en cada red Fabric, puede seleccionar las ranuras que activará. Por ejemplo, si se activa la red Fabric A, las ranuras activadas tendrán la función FlexAddress activada solo en la red Fabric A. Las demás redes usan la dirección WWN/MAC asignada de fábrica en el servidor.

Seleccione las ranuras que tienen la función FlexAddress en todas las redes Fabric activadas. Por ejemplo, no es posible activar las redes Fabric A y B y activar la función 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).

Enlaces relacionados

Encendido en LAN con FlexAddress
Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis
Configuración de FlexAddress para las ranuras en el nivel del servidor
Configuración adicional de FlexAddress para Linux

Encendido en LAN con FlexAddress

Cuando se implementa la función FlexAddress por primera vez en un módulo del servidor, se requiere de una secuencia de apagado y encendido para que FlexAddress se active. FlexAddress en dispositivos Ethernet se programa por el BIOS del módulo del servidor. Para que el BIOS del módulo del servidor programe la dirección, necesita estar en funcionamiento, lo que requiere que el módulo del servidor se encienda. Cuando se completan las secuencias de apagado y encendido, las identificaciones MAC asignadas por el chasis están disponibles para la función de encendido en LAN (WOL).

Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis

En el nivel del chasis, puede activar o desactivar la función FlexAddress para las redes Fabric y las ranuras. FlexAddress se activa para cada red Fabric y luego se seleccionan las ranuras que deben participar en la función. Tanto las redes Fabric como las ranuras deben activarse para configurar FlexAddress satisfactoriamente.

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, diríjase a **Descripción general del servidor** y haga clic en **Configuración → FlexAddress**.
   Aparecerá la página **Implementar FlexAddress**.
2. En la sección **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, anule la selección.

   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 **Activado** para la ranura en la cual desea activar FlexAddress. Para desactivar esta opción, anule la selección.

   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#> = 1 or 16` y `<state> = 0 or 1`

El valor 0 es desactivar y 1 es activar.

Para obtener más información sobre el comando **setflexaddr**, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)* 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 <n.° de ranura> <estado>] [-f <nombre_de red_Fabric>
<estado>]
```

donde, `<n.° de ranura>= de 1 a 16`

`<nombre_de red_Fabric> =A, B, C`

`<estado> = 0 o 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 (RHEL) y RHEL 5: ejecute Kudzu, una utilidad para detectar y configurar hardware nuevo o cambiado en el sistema. Kudzu muestra el menú de detección de hardware, que detecta el cambio en la dirección MAC ya que se quitó y agregó hardware.

Visualización de las identificaciones World Wide Name/Media Access Control (WWN/MAC)

La página **Resumen de WWN/MAC** permite ver la configuración de WWN y la dirección MAC de una ranura en el chasis.

Configuración de la red Fabric

La sección **Configuración de la red Fabric** muestra el tipo de red Fabric de entrada/salida que se instala para la red Fabric A, red Fabric B y red Fabric C. Una marca verde indica que la red Fabric está activada para FlexAddress. La función FlexAddress se utiliza para instalar direcciones WWN/MAC de ranuras persistentes y asignadas por el chasis en varias redes Fabric y ranuras en el chasis. Esta función se activa por red Fabric y por ranura.

NOTA: Para obtener más información acerca de la función FlexAddress, consulte CMCNoble_About Flexaddress.

Direcciones WWN/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.

- **Ubicación** muestra la ubicación de la ranura ocupada por los módulos de entrada/salida. Las seis ranuras se identifican mediante una combinación del nombre del grupo (A, B o C) y el número de ranura (1 o 2); entonces los nombre de ranuras son 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 **Asignadas por el servidor** o **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 persistentes de ranura. Cuando se seleccionan 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 32. Comandos y mensajes de salida de FlexAddress

Situación	Comando	Mensaje de 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`
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 todo el software que se distribuye con el producto Dell, para el que no existe un contrato de licencia diferente entre usted y el fabricante o el propietario del software (de manera colectiva, el "Software"). Este contrato no es para la venta de Software o de cualquier otra propiedad intelectual. Todos los derechos de título y propiedad intelectual del Software y para este pertenecen al fabricante o propietario del Software. Todos los derechos no otorgados expresamente bajo este contrato son derechos reservados por el fabricante o propietario del Software. Al

abrir o romper el sello de los paquetes de Software, instalar o descargar el Software, o utilizar el Software que se ha cargado previamente o que se incluye en el producto, usted acepta estar sujeto a los términos de este contrato. Si no acepta estos términos, devuelva de inmediato todos los artículos de Software (discos, material escrito y embalaje) y elimine el Software cargado previamente en el producto o incorporado en él.

Únicamente podrá utilizar una copia de Software por equipo a la vez. Si dispone de varias licencias de Software, podrá utilizar en cualquier momento tantas copias como licencias tenga. Con el término "utilizar" se entiende cargar el Software en la memoria temporal o en el almacenamiento permanente del equipo. La instalación del Software en un servidor de red con el único fin de distribuirlo a otros equipos no significará "utilizarlo" siempre y cuando disponga de una licencia independiente para cada equipo en el que 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 que disponga. Si la cantidad de usuarios del Software instalado en un servidor de red supera el número de licencias, deberá adquirir licencias adicionales hasta que la cantidad de licencias iguale la cantidad de usuarios, antes de permitir que estos utilicen el Software. Si usted es un cliente comercial de Dell o un socio de Dell, por el presente concede a Dell o a un representante seleccionado por Dell, el derecho a realizar una auditoría sobre el uso que usted hace del Software durante el horario laboral normal, acepta cooperar con Dell en dicha auditoría y proporcionarle todos los informes relacionados razonablemente con el uso que hace del Software. La auditoría se limitará a la verificación del cumplimiento de los términos de este contrato por su parte.

El Software está protegido por las leyes de derechos de autor de Estados Unidos y por tratados internacionales. Únicamente podrá hacer una copia del Software para disponer de una copia de seguridad o para archivarlo o transferirlo a un solo disco duro, siempre que guarde el original solo para fines de respaldo o de archivado. No puede alquilar o arrendar el software 240 mediante FlexAddress y las tarjetas FlexAddress Plus ni copiar los materiales impresos que se adjuntan con él, pero sí puede transferir el software y todos los materiales adjuntos de manera permanente como parte de la venta o transferencia del producto Dell siempre y cuando no se quede con ninguna copia y los destinatarios acepten los términos de este documento. Cualquier transferencia deberá incluir la actualización más reciente y todas las versiones anteriores. No se permite aplicar técnicas de ingeniería inversa, descompilar o desensamblar el Software. Si el paquete que acompaña a su equipo contiene CD, disquetes de 3.5" o de 5.25", podrá utilizar únicamente los adecuados para su equipo. No podrá utilizar los discos en otro equipo o red, ni prestarlos, alquilarlos, arrendarlos o transferirlos a otro usuario, salvo según lo permita el presente contrato.

GARANTÍA LIMITADA

Dell garantiza que los discos de Software no presentarán defectos en los materiales ni en su fabricación, siempre que se realice un uso normal, durante noventa (90) días a partir de la fecha de recepción. Esta garantía se limita a usted y no es transferible. Las garantías implícitas se limitan a noventa (90) días a partir de la fecha de recepción del Software. En algunas jurisdicciones no existen limitaciones en la vigencia de la garantía implícita, de modo que esta limitación puede no ser aplicable en su caso. La responsabilidad total de Dell y de sus proveedores, así como su remedio exclusivo, se limitará (a) a la devolución del importe pagado por el Software o (b) a la sustitución de los discos que no cumpla esta garantía y que usted envíe a Dell con un número de autorización de devolución, por su cuenta y riesgo. Esta garantía limitada se anulará si se daña el disquete como resultado de accidentes, abuso, usos incorrectos, tareas de mantenimiento o modificaciones por parte de alguna persona que no pertenezca a Dell. La garantía cubre los discos de reemplazo durante el período restante de la garantía original o durante treinta (30) días, lo que resulte mayor.

Dell NO garantiza que las funciones del Software satisfarán sus necesidades o que el funcionamiento del Software no se interrumpirá o no tendrá errores. Usted asume la responsabilidad de seleccionar el Software para lograr los resultados que espera, así como del uso y de los resultados obtenidos con el Software.

DELL, EN SU NOMBRE Y EN EL DE SUS PROVEEDORES, NO SE HARÁ RESPONSABLE DE NINGUNA OTRA GARANTÍA, EXPLÍCITA O IMPLÍCITA, INCLUYENDO PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO, POR LO QUE SE REFIERE AL SOFTWARE Y A TODOS LOS MATERIALES ESCRITOS QUE LO ACOMPAÑAN. Esta garantía limitada le otorga derechos legales específicos; es posible que usted tenga otros derechos, que varían en función de la jurisdicción.

EN NINGÚN CASO DELL O SUS PROVEEDORES SERÁN RESPONSABLES DE LOS DAÑOS QUE PUEDAN OCURRIR (LO QUE INCLUYE, SIN LÍMITE, LOS DAÑOS POR PÉRDIDA DE BENEFICIOS, INTERRUPCIÓN O PÉRDIDA DE INFORMACIÓN DEL NEGOCIO O CUALQUIER OTRA PÉRDIDA PECUNIARIA) A CAUSA DEL USO O LA INCAPACIDAD DE UTILIZAR EL

SOFTWARE, AUNQUE SE LE NOTIFIQUE DE LA POSIBILIDAD DE TALES DAÑOS. Puesto que algunas jurisdicciones no permiten la exclusión o limitación de responsabilidad por daños resultantes o accidentales, la limitación anteriormente mencionada puede no ser aplicable en su caso.

SOFTWARE DE CÓDIGO DE FUENTE ABIERTO

Una parte de este CD puede contener software de código de fuente abierto, que puede utilizar bajo los términos y condiciones de la licencia específica bajo la cual el software se distribuye.

ESTE SOFTWARE DE CÓDIGO DE FUENTE ABIERTO SE DISTRIBUYE CON LA INTENCIÓN DE QUE PUEDA SER ÚTIL, PERO SE PROPORCIONA "TAL CUAL" SIN NINGUNA GARANTÍA EXPLÍCITA O EXPRESA; INCLUYENDO PERO SIN LIMITARSE A LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O IDONEIDAD PARA UN FIN ESPECÍFICO. BAJO NINGUNA CIRCUNSTANCIA, DELL, LOS TITULARES DE LOS DERECHOS DE AUTOR O LOS CONTRIBUYENTES SE HARÁN RESPONSABLES DE DAÑOS DIRECTOS, INDIRECTOS, ACCIDENTALES, ESPECIALES, EJEMPLARES O CONSECUENTES (LO QUE INCLUYE, SIN LIMITARSE A, LA ADQUISICIÓN DE SERVICIOS O PRODUCTOS SUSTITUTOS; PÉRDIDA DE USO, DATOS O BENEFICIOS; O LA INTERRUPCIÓN DEL NEGOCIO) SIN IMPORTAR LA MANERA EN QUE SE HAYAN PRODUCIDO NI LA TEORÍA DE RESPONSABILIDAD, YA SEA BAJO CONTRATO, RESPONSABILIDAD ESTRICTA O DELICTIVA (LO QUE INCLUYE LA NEGLIGENCIA O SIMILARES) 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 constituyen "software informático comercial" y "documentación de software informático comercial" según 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 permanecerá vigente hasta que finalice. Dicha finalización se llevará a cabo según las condiciones estipuladas anteriormente o si usted no cumple alguno de estos términos. Una vez que haya finalizado, usted acepta que procederá a la destrucción del Software y de los materiales que lo acompañan, así como de todas las copias de estos. Este contrato está regulado por las leyes del estado de Texas. Las cláusulas de este contrato son independientes. 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 cualquier derecho a juicio con jurado con respecto al Software o a este contrato. Como esta renuncia de derechos puede no ser efectiva en ciertas jurisdicciones, es posible que no se aplique en su caso. Usted reconoce que ha leído el presente contrato, que lo entiende y acepta estar sujeto a sus términos, y que esta es la declaración completa y exclusiva del contrato entre usted y Dell con respecto al Software.

13

Administración de la red Fabric de E/S

El chasis puede tener hasta seis módulos de E/S (IOM), donde cada módulo de E/S es de paso o conmutación. Los módulos de E/S se clasifican en tres grupos: A, B y C. Cada grupo tiene dos ranuras: Ranura 1 y Ranura 2.

Las ranuras están diseñadas con letras, de izquierda a derecha, en la parte posterior del chasis: A1 | B1 | C1 | C2 | B2 | A2. Cada servidor tiene dos ranuras para dos tarjetas mezzanine (MC) para conectar los módulos de E/S. La MC y el módulo de E/S correspondiente deben tener la misma red Fabric.

El sistema de E/S del chasis está dividido en tres rutas de datos discretas: A, B y C. Estas rutas se describen como redes FABRIC y admiten Ethernet, Fibre Channel o InfiniBand. Estas rutas discretas de red Fabric se dividen en dos bancos de E/S, banco uno y banco dos. Cada adaptador de E/S de servidor (tarjeta Mezzanine o LOM) puede tener dos o cuatro puertos según la capacidad. Estos puertos están divididos en forma pareja con respecto a los bancos de módulos de E/S uno y dos para permitir redundancia. Cuando se implementan redes Ethernet, iSCSI o FibreChannel, se expanden sus enlaces redundantes en los bancos uno y dos para obtener máxima disponibilidad. El módulo de E/S discreto se identifica con el identificador de red Fabric y el número de banco.

Ejemplo: A1 denota red Fabric A en banco 1. C2 denota red Fabric C en banco 2.

El chasis admite tres tipos de red Fabric o protocolo. Los módulos de E/S y las tarjetas Mezzanine de un grupo deben tener los mismos tipos de red Fabric o tipos compatibles.

- Los módulos de E/S del Grupo A siempre están conectados a los adaptadores Ethernet integrados de los servidores; por lo tanto, el tipo de red Fabric del grupo A siempre será Ethernet.
- En el Grupo B, las ranuras de los módulos de E/S están conectadas permanentemente a la primera ranura MC de cada módulo del servidor.
- En el Grupo C, las ranuras de los módulos de E/S están conectadas permanentemente a la segunda ranura MC de cada módulo del servidor.

NOTA: En la CLI del CMC, se hace referencia a los módulos de E/S mediante la convención conmutador-n: A1=conmutador-1, A2=conmutador-2, B1=conmutador-3, B2=conmutador-4, C1=conmutador-5 y C2=conmutador-6.

Enlaces relacionados

Descripción general de la administración de redes Fabric
Configuraciones no válidas
Situación de encendido por primera vez
Supervisión de la condición del módulo de E/S
Configuración de los valores de red para módulos de E/S
Administración de VLAN para módulos de E/S
Administración de las operaciones de control de alimentación para módulos de E/S
Activación o desactivación del parpadeo del LED para los módulos de E/S
Restablecimiento de los módulos de E/S a la configuración predeterminada de fábrica

Descripción general de la administración de redes Fabric

La administración de redes Fabric ayuda a evitar problemas relacionados con la electricidad, la configuración o la conectividad debido a la instalación de un módulo de E/S o MC que tiene un tipo de red Fabric no compatible 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 las 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 está indicada por su número de grupo (A, B o C). Estas rutas de redes Fabric discretas están divididas en dos bancos de E/S, banco uno y dos. En el chasis, los nombres de las ranuras de E/S están identificados como A1, A2, B1, B2, C1 y C2.

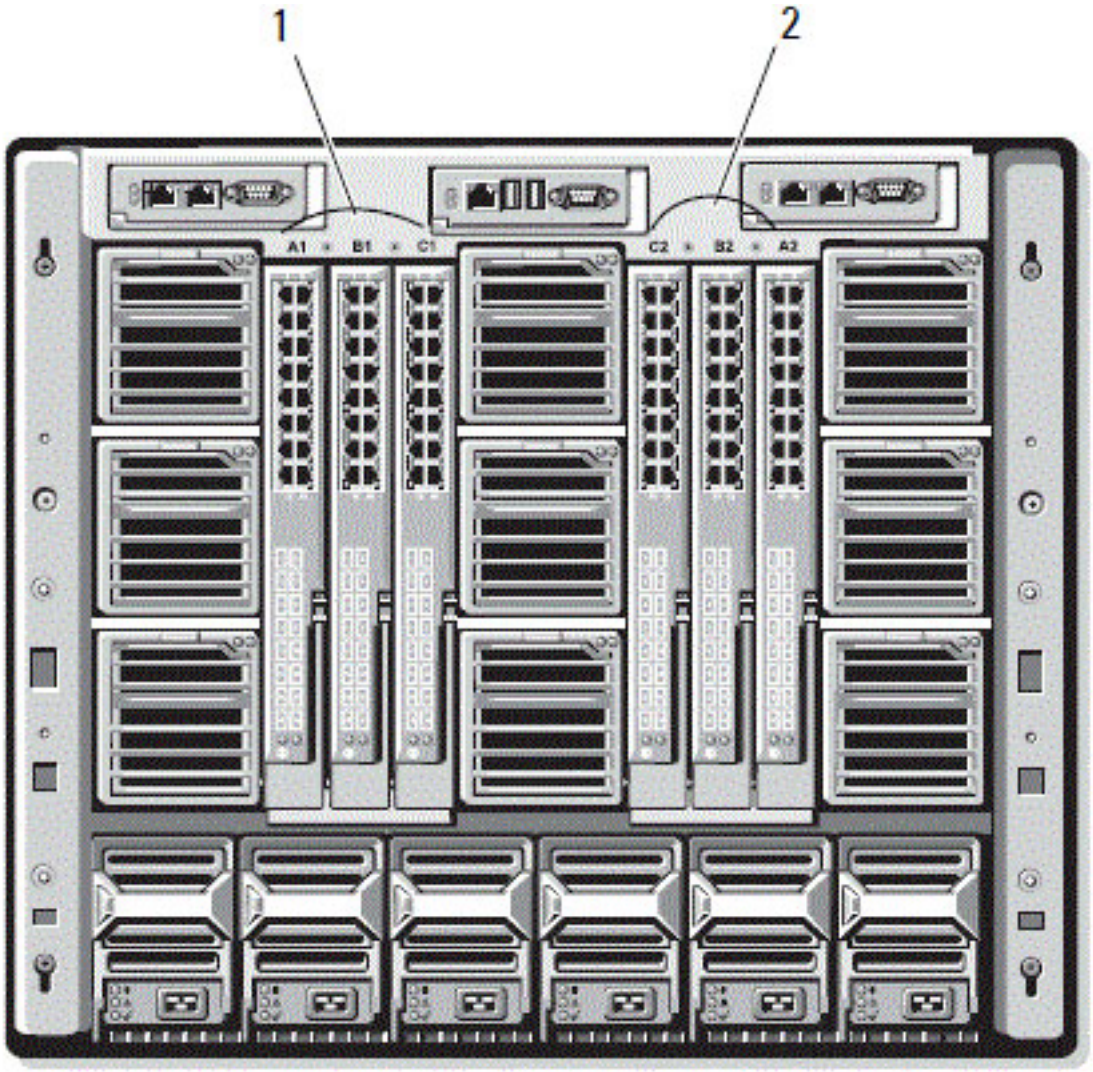


Ilustración 4. Vista posterior de un chasis, que muestra la ubicación de los módulos de E/S

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 de Ethernet conectada a un módulo de E/S de Fibre Channel es una configuración no válida. No obstante, una MC de Ethernet conectada a un conmutador de Ethernet y a un módulo de E/S de paso de Ethernet instalado en el mismo grupo de módulos de E/S es una conexión válida.

- Un módulo de E/S de paso de Fibre Channel y un módulo de E/S de conmutador de fibre channel en las ranuras B1 y B2 es una configuración válida si las primeras MC en todos los servidores son también de fibre channel. En este caso, el CMC se enciende en los módulos de E/S y los servidores. No obstante, es posible que el software de redundancia de fibre channel no admita esta configuración; no todas las configuraciones válidas son necesariamente configuraciones admitidas.

  La verificación de redes Fabric para los módulos de E/S y MC de servidores se realiza solo cuando el chasis está encendido. Cuando el chasis está en estado de espera, los iDRAC en los módulos del servidor permanecen apagados y de este modo no pueden informar el tipo de red Fabric de MC del servidor. Es posible que el tipo de red Fabric de MC no se informe en la interfaz de usuario de CMC hasta que el iDRAC en el servidor esté encendido. Además, si el chasis está encendido, la verificación de redes Fabric se realiza cuando un servidor o módulo de E/S se inserta (opcional). Si se detecta una incompatibilidad de redes Fabric, el servidor o módulo de E/S puede encenderse y el LED de estado aparecerá intermitente en color ámbar.

Configuraciones no válidas

Hay tres tipos de configuraciones no válidas:

- Configuración no válida entre la MC y el módulo de E/S, donde un tipo de red Fabric instalado recientemente o el servidor son diferentes de la red Fabric del módulo de E/S existente; es decir, que el módulo de E/S o la MC de un solo servidor no es compatible con el módulo de E/S correspondiente. En este caso, el resto de los servidores del chasis están en ejecución, pero el servidor con la tarjeta MC incompatible no puede encenderse. El botón de encendido del servidor parpadea de color ámbar para alertar sobre la incompatibilidad de la red Fabric.
- Configuración no válida entre la MC y el módulo de E/S, donde el tipo de red Fabric recientemente instalada del módulo de E/S y los tipos de redes Fabric de la MC residente no coinciden o son incompatibles. El módulo de E/S incompatible se mantiene en el estado apagado. El CMC agrega una entrada al CMC y el hardware se registra observándose la configuración no válida y especificando el nombre del módulo de E/S. El CMC hace que la pantalla LED de error parpadee en el módulo de E/S incorrecto. Si el CMC está configurado para enviar alertas, enviará alertas de correo electrónico y SNMP por este suceso.
- Configuración no válida entre los módulos de E/S, donde un módulo de E/S recientemente instalado tiene un tipo de red Fabric incompatible o diferente de un módulo de E/S ya instalado en su grupo. El CMS mantiene el módulo de E/S recientemente instalado en estado apagado, hace que la pantalla LED de error del módulo de E/S parpadee y registra las entradas en el CMC y los registros de hardware sobre la incompatibilidad.

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 en cada grupo encenderse antes que los demás. En este momento no se realiza ninguna verificación de los tipos de red Fabric. Si no hay ningún módulo de E/S en la primera ranura de un grupo, se enciende el módulo que está en la segunda ranura de ese grupo. Si ambas ranuras tienen módulos de E/S, se compara el módulo en la segunda ranura con el módulo que está en 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 módulo de paso y uno de conmutación en el mismo grupo, siempre y cuando sus redes Fabric sean idénticas. Los módulos de conmutación y de paso pueden existir en el mismo grupo, incluso si fueron fabricados por proveedores distintos.

Supervisión de la condición del módulo de E/S

Para obtener información sobre 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 del enlace ascendente y del enlace descendente del módulo de E/S con 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.
   Aparecerá la página **Estado del módulo de E/S** específica de la ranura del módulo de E/S. Aparecerán las tablas **Estado del enlace ascendente del módulo de E/S** y **Estado del enlace descendente del módulo de E/S**. Estas tablas muestran información sobre los puertos de enlace descendente (1–32) 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 esté activo. Esta página muestra el estado del agregador de E/S. Si el estado es inactivo, esto implica que los puertos de los servidores en el agregador de E/S pueden estar inactivos debido a configuraciones no válidas.

Visualización de la información de la sesión de FCoE del módulo de E/S con 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 desea ver y haga clic en **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 E/S 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 del apilamiento: esto identifica la función de este módulo en el apilamiento. Los valores válidos son Maestro, Miembro y 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 referida al comando **racadm getioinfo** en *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*.

Configuración de los valores de red para módulos de E/S

Es posible especificar los valores de red para la interfaz usada 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 sobre el módulo de E/S para la dirección IP de administración en banda predeterminada.

NOTA: No intente configurar los valores de la red del módulo de E/S para módulos de paso de Ethernet y conmutadores de Infiniband.

Configuración de los valores de red para los módulos de E/S mediante la interfaz web del CMC

NOTA: Esta función está admitida solamente en el módulo de E/S del conmutador de agregación de E/S PowerEdge. 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 del CMC:

1. En el árbol del sistema, vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración** o expanda **Descripción general del módulo de E/S**, 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 el módulo de E/S requerido, 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 para el CMC)*.

NOTA: La dirección IP establecida en los módulos de E/S a partir del CMC no se guarda en la configuración de inicio permanente del conmutador. Para guardar la configuración de la dirección IP de forma permanente, debe introducir el comando `connect switch-n` o el comando de RACADM `racadm connect switch -n` o bien, usar una interfaz directa a la interfaz gráfica de usuario del módulo de E/S para guardar esta dirección en el archivo de configuración de inicio.

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 establecer la configuración de red de los módulos de E/S mediante RACADM, debe establecer la fecha y la hora. Consulte la sección del comando **deploy** en *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

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 está admitida solamente en el módulo de E/S del conmutador de agregación de E/S PowerEdge. No se admiten otros módulos de E/S, como MXL 10/40GbE.

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

1. En el árbol del sistema, vaya a **Descripción general del módulo de E/S** y haga clic en **Configuración** o expanda 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.

Enlaces relacionados

Descripción general de la administración de redes Fabric
Configuraciones no válidas
Situación de encendido por primera vez
Supervisión de la condición del módulo de E/S
Configuración de los valores de red para módulos de E/S
Administración de VLAN para módulos de E/S

Administración de las operaciones de control de alimentación para módulos de E/S
Activación o desactivación del parpadeo del LED para los módulos de E/S

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

Puede actualizar el software del módulo de E/S al seleccionar la imagen de software requerida en una ubicación especificada. También puede regresar a una versión de software anterior.

NOTA: Esta función está admitida solamente en el módulo de E/S del conmutador de agregación de E/S PowerEdge. 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 del CMC:

1. Vaya a **Descripción general del chasis → Descripción general del módulo de E/S → Actualizar**
   Aparecerá la página **Firmware y software de 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 **Firmware y software de módulo de E/S**.
2. En la página **Firmware y software de módulo de E/S**, dentro de la sección **Software de E/S**, seleccione la columna **Actualizar** para el módulo de E/S para el que desea actualizar el software y haga clic en **Aplicar actualización de software**.
   Otra opción es regresar a versiones anteriores del software; para ello, seleccione la casilla de la columna **Revertir**.
3. Seleccione la imagen de software para la actualización de software, utilizando la opción **Explorar**. El nombre de la imagen de software se visualiza en el campo **Ubicación de software de módulo de E/S**.
   La sección **Estado de actualización** proporciona información sobre el estado de la actualización o reversión de software. Aparecerá un indicador de estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar según la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización de firmware.

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

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

   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**.

Administración de VLAN para módulos de E/S

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

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

Enlaces relacionados

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. El 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 (Prioridad)

NOTA:

La configuración de la VLAN de administración en la página **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 A, B o C específica.

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 **Módulos de E/S**, active la red VLAN para los módulos de E/S, establezca la prioridad y especifique la identificación. Para obtener más información sobre los campos, consulte *CMC Online Help (Ayuda en línea para el 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 de 1 a 6.

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

  Los valores válidos para `<VLAN priority>` (<Prioridad de VLAN>) son de 0 a 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 de 1 a 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: Es posible configurar los valores de VLAN solo en el módulo de E/S del agregador de módulos de E/S PowerEdge. No se admiten otros módulos de E/S que incluyen MXL 10/40GbE.

Para configurar los valores de VLAN en 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**.

   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 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**, escriba las identificaciones de VLAN para los módulos de E/S. Proporcione las identificaciones de VLAN en el rango de 1 a 4094. Las identificaciones de VLAN pueden escribirse 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: La sección Resumen de VLAN de todos los puertos muestra información sobre los módulos de E/S presentes en el chasis y las VLAN asignadas. Haga clic en Guardar para guardar un archivo csv del resumen de la configuración actual de VLAN.

   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 **Apply (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 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**.

   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 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 **Editar VLAN**, seleccione **Mostrar VLAN** en la lista desplegable y haga clic en **Aplicar**.

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

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 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 **Agregar VLAN etiquetadas** en la lista desplegable y haga clic en **Aplicar**.

   Las VLAN etiquetadas se asignan a los módulos de E/S seleccionados.

   Se mostrará el mensaje de operación correcta. La configuración actual de VLAN asignada a los módulos de E/S se muestra en el campo **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 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 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.

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

Actualización de VLAN sin etiquetar para módulos de E/S mediante la interfaz web 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 **Aceptar** para confirmar.

   Las VLAN sin etiquetar se actualizarán con las configuraciones de la VLAN sin etiquetar recientemente asignada.

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

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 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 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 **Aceptar** para confirmar.

   Las VLAN se asignarán a los módulos de E/S seleccionados de acuerdo con las configuraciones predeterminadas.

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

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. Este módulo opcional de acoplamiento activo para el chasis ofrece acceso local de teclado, mouse y video a los servidores del chasis y a la línea de comandos del CMC activo.

Enlaces relacionados

Interfaz de usuario del iKVM
Funciones clave de iKVM
Interfaces de conexión física

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. La interfaz OSCAR permite seleccionar uno de los servidores o la línea de comandos del CMC de Dell a los que se desea acceder por medio del teclado, la pantalla y el mouse locales. Se permite solo una sesión de iKVM por chasis.

Enlaces relacionados

Uso de la interfaz OSCAR

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 tanto 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: el CMC asigna nombres de ranuras únicos 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 el 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 del CMC, consulte Configuring Slot Names (Configuración de nombres de las ranuras). Para cambiar el nombre de una ranura mediante RACADM, consulte la sección **setslotname** en *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*.
- 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 del CMC o el comando `fwupdate` de RACADM.

Enlaces relacionados

Uso de la interfaz OSCAR
Administración de servidores con iKVM

Administración del iKVM desde el CMC
Actualización de firmware del iKVM

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 frontal.

Prioridades de las conexiones del iKVM

Solo hay una conexión del 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 conexión 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 existen conexiones de iKVM en el panel frontal y la ACI, la conexión del panel frontal permanecerá activa y la otra quedará desactivada. Si existen conexiones del panel posterior y de la ACI, estas últimas tendrán prioridad.

Categorización por medio de la conexión de ACI

El iKVM admite conexiones categorizadas con servidores y la consola de línea de comandos del 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.

Enlaces relacionados

Inicio de OSCAR
Conceptos básicos de navegación
Configuración de OSCAR

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 la interfaz OSCAR. Puede activar una, varias o todas las secuencias de teclas; para ello, marque las casillas en la sección Invocar OSCAR del cuadro de diálogo Principal.

Enlaces relacionados

Configuración de la seguridad de la consola
Conceptos básicos de navegación

Conceptos básicos de navegación

Tabla 33. : 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 la interfaz OSCAR según los valores de la sección **Invocar OSCAR**. Puede activar dos, tres o todas las secuencias de teclas; para ello, active las casillas de la sección **Invocar OSCAR** en el cuadro de diálogo **Principal** y haga clic en **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 editarlo y activa las teclas de flecha izquierda y derecha para desplazar el cursor. Presione <Intro> nuevamente para salir del modo Editar.

Tecla o secuencia de teclas	Resultado
<Impr Pant>, <Retroceso>	Vuelve a la selección anterior si no hubo otras pulsaciones de teclas.
<Impr Pant>, <Alt>+<0>	Desconecta a un usuario de un servidor inmediatamente; no se selecciona ningún servidor. El indicador de estado muestra la palabra "Libre" (esta acción solo se aplica a la tecla =<0> del teclado principal, no 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>	Está desactivada. 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**.

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.

Enlaces relacionados

Cambio de comportamiento del modo de visualización

Asignación de secuencias de teclas para OSCAR
Configuración del tiempo de retraso de la pantalla en la interfaz OSCAR
Configuración de la visualización del indicador de estado

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 **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 **Invocar OSCAR** y haga clic en **Aceptar**. La tecla predeterminada para la invocación de 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.

Enlaces relacionados

Conmutación mediante software

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 Indicador para configurar el indicador que desea mostrar para cada servidor o para cambiar el color, la opacidad, la imagen, la duración y la ubicación del indicador en el escritorio.

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 **Color de visualización**, seleccione un color de 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  .

Administración de servidores con iKVM

El iKVM es una matriz de conmutación analógica que admite hasta 16 servidores. El conmutador iKVM utiliza la interfaz de usuario OSCAR para seleccionar y configurar los servidores. Además, incluye una entrada de sistema que permite establecer una conexión de consola de línea de comandos del CMC con el CMC.

Si existe una sesión de redirección de consola activa y hay un monitor de menor resolución conectado con el iKVM, la resolución de la consola del servidor puede restablecerse si el servidor se selecciona en la consola local. Si el servidor ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Si presiona <Ctrl><Alt><F1> en el iKVM, se cambiará de Linux a consola de texto.

Enlaces relacionados

Compatibilidad con periféricos
Visualización y selección de servidores

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 admitidos. El iKVM no admite datos transmitidos desde otros periféricos USB.

Visualización y selección de servidores

Cuando inicia OSCAR, aparece el cuadro de diálogo **Principal**. Utilice el cuadro de diálogo **Principal** para ver, configurar y administrar servidores a través del iKVM. Puede ver los servidores por nombre o por ranura. El número de ranura corresponde al número de ranura del chasis en la que se encuentra el servidor. La columna **Ranura** indica el número de ranura en la que está instalado un servidor.

NOTA: La línea de comandos del CMC de Dell ocupa la ranura 17. Si selecciona esta ranura se mostrará la línea de comandos del CMC, donde podrá ejecutar comandos de RACADM o conectarse a la consola serie del servidor o a módulos de E/S.

NOTA: A los nombres y los números de ranura de los servidores los asigna el CMC.

Enlaces relacionados

Conmutación mediante software
Visualización del estado del servidor
Selección de servidores

Visualización del estado del servidor

Las columnas ubicadas en el lado derecho del cuadro de diálogo **Principal** indican el estado del servidor en el chasis. En la siguiente tabla se describen los símbolos de estado.

Tabla 34. 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

Use el cuadro de diálogo **Principal** para seleccionar 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 el servidor anterior, presione <Impr Pant> y después <Retroceso>. Estas combinaciones de teclas permiten alternar entre las conexiones actual y 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 después <Alt><0>. De esta forma el estado queda libre, sin servidores seleccionados. Si el indicador de estado del escritorio está activo, mostrará el estado Libre. Consulte **Setting Status Flag Display (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. Puede realizar una conmutación por software a un servidor pulsando <Impr Pant> y luego escribiendo los primeros caracteres de su nombre o número. Si anteriormente definió un tiempo de retraso (la cantidad de segundos que transcurren antes de que el cuadro de diálogo **Principal** aparezca al presionar <Impr Pant>) y presiona la secuencia de teclas antes de que finalice ese plazo, la interfaz OSCAR no se abrirá.

Enlaces relacionados

Configuración de la conmutación mediante software
Conmutación mediante software a un servidor

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 **Aceptar**.

Conmutación mediante software a un servidor

Para realizar una conmutación mediante software a un servidor:

- Seleccione un servidor presionando <Impr Pant>. Si los servidores aparecen ordenados por ranura según la opción elegida (es decir, si el botón 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 KVM y de ACI en el panel posterior están desactivadas. Si el monitor se desactiva (es decir, si se quita del panel frontal o se desactiva mediante un comando del CMC), la conexión de ACI se activará y la conexión de KVM permanecerá desactivada.

Enlaces relacionados

Prioridades de las conexiones del iKVM

Activación o desactivación del acceso al iKVM desde el panel frontal

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 del iDRAC, el usuario remoto puede desactivar la consola local en la interfaz web del iDRAC. El usuario del iKVM local ve un mensaje de protocolo OSCAR indicando que se apropió la conexión en una cantidad de tiempo determinada. El usuario local debería terminar de usar la consola antes de que finalice la conexión iKVM con el servidor.

No existe una función de apropiación disponible para el usuario del iKVM.

NOTA: Si un usuario remoto del iDRAC desactivó el video local de un servidor específico, 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 OSCAR para indicar que se encuentra bloqueado o no disponible para uso local. Consulte Viewing Server Status (Visualización del estado del servidor).

Enlaces relacionados

Visualización del estado del servidor

Configuración de la seguridad de la consola

OSCAR 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, 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.

Enlaces relacionados

Acceso al cuadro de diálogo Seguridad
Configuración de la contraseña
Protección por contraseña de la consola
Configuración de la desconexión automática
Eliminación de la protección por contraseña de la consola
Activación del modo de protector de pantalla sin contraseña
Salida del modo de protector de pantalla
Eliminación de una contraseña perdida u olvidada

Acceso al cuadro de diálogo Seguridad

Para obtener acceso 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 y presione <Intro>. Las contraseñas distinguen entre mayúsculas y minúsculas y deben tener entre 5 y 12 caracteres. Deben incluir al menos una letra y un número. Los caracteres permitidos son: letras de la A–Z, a–z, números del 0–9, espacios y guiones.
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 define el modo en **Energía**, el monitor entrará en modo inactivo. Por lo general, para indicar este estado el monitor se apaga y una luz de color ámbar reemplaza al LED de alimentación de color verde.
   - Si se define el modo en **Pantalla**, el indicador OSCAR se desplazará 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 de energía puede dañar un monitor no compatible con ENERGY STAR. No obstante, una vez comenzada la prueba es posible cerrarla de inmediato mediante la interacción del teclado o del 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 **Prueba**. Aparecerá el cuadro de diálogo **Prueba de protector de pantalla**. Haga clic en **Aceptar** para iniciar la prueba.

   La prueba dura 10 segundos. Al finalizar, la pantalla regresará al cuadro de diálogo **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 **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 **Principal**, haga clic en **Configuración** y después en **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 **Aceptar**.

Activación del modo de protector de pantalla sin contraseña

NOTA: Si la consola está protegida con contraseña, primero se 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 **Prueba**. Aparecerá el cuadro de diálogo **Prueba de protector de pantalla**. Haga clic en **Aceptar** para iniciar la prueba.

   La prueba demora 10 segundos. Una vez completada, aparecerá el cuadro de diálogo **Seguridad**.

   NOTA: La activación del modo **Protector de pantalla** desconecta al usuario de un servidor. Esta acción significa que no hay seleccionado ningún servidor. El indicador de estado muestra **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 restablecerla a los valores predeterminados de fábrica de iKVM y, a continuación, cambiar la contraseña. Puede restablecer la contraseña mediante la interfaz web del 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**.

Es posible cambiar la contraseña predeterminada mediante OSCAR. Para obtener más información, consulte Setting Password (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 Activación del panel frontal y Activación de Dell CMC Console, si difieren de los valores predeterminados.

Para obtener más información sobre el subcomando `racresetcfg`, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

Cambio de idioma

Use el cuadro de diálogo **Idioma** para cambiar el texto de OSCAR que aparece en alguno de los idiomas admitidos. 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 muestra el cuadro de diálogo **Versión**. La mitad superior del cuadro de diálogo **Versión** enumera las versiones del subsistema.
3. Haga clic en la  o presione <Esc> para cerrar el cuadro de diálogo **Versión**.

Exploración del sistema

En el modo de exploración, el iKVM explora automáticamente cada ranura (cada servidor). Es posible explorar hasta 16 servidores y especificar los que se desea explorar y la cantidad de segundos que cada servidor se mostrará.

Enlaces relacionados

Incorporación de servidores a la lista de exploración:
Eliminación de un servidor de la lista de exploración
Inicio del modo de exploración
Cancelación del modo de exploración

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 **Aceptar**.
   Aparecerá un mensaje para indicar que el mouse y el teclado fueron restablecidos.
5. Haga clic en la  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.
   Aparecerá 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 más de un servidor del sistema a la vez para asegurarse de que todos los servidores seleccionados reciban la misma señal de entrada. 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 para todos los servidores que reciben la transmisión de modo que la interpretación de las pulsaciones sea la misma. Específicamente, los modos <Bloq Mayús> y <Bloq Núm> deben ser iguales en todos los teclados. Mientras el iKVM intenta enviar pulsaciones de teclas a la vez a todos los servidores seleccionados, algunos servidores pueden inhibirse y retrasar la transmisión.

- Transmisión de movimientos del mouse: para que el mouse funcione correctamente, todos los servidores deben tener los mismos 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. Dado que es muy difícil cumplir estas condiciones, la transmisión de movimientos del 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. Después 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 **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 **Aceptar** para activar la transmisión. Para cancelar y regresar al cuadro de diálogo **Comandos** haga clic en la  o presione <Esc>.
9. Si la transmisión está activada, escriba la información o ejecute los movimientos del mouse que desea transmitir desde la estación de administración. Sólo se podrá acceder a los servidores de la lista.

Administración 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 Dell CMC Console

Enlaces relacionados

Actualización de firmware del iKVM
Activación o desactivación del acceso al iKVM desde el panel frontal
Visualización de información y estado de condición del iKVM
Activación del acceso al iKVM desde Dell CMC Console

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 activarla, seleccione la opción **USB/Video del panel frontal activado**. Para desactivarla, borre la opción **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 <valor>
```

donde <valor> es 1 (activar) o es 0 (desactivar). Para obtener más información acerca del subcomando

```
config
```

consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

Activación del acceso al iKVM desde Dell CMC Console

Para activar el acceso a la CLI del CMC desde iKVM mediante la interfaz web del CMC, en el árbol del sistema, vaya a **Descripción general del chasis** → **iKVM** y haga clic en la ficha **Configuración**. Seleccione la opción **Permitir acceso a la CLI del CMC desde iKVM** y haga clic en **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
```

Enlaces relacionados

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

15
Administración y supervisión de la alimentación

El gabinete de servidor Dell PowerEdge M1000e es el servidor modular más eficiente en términos de alimentación. Su diseño permite incluir ventiladores y suministros de energía de alta eficacia y está optimizado para que el aire circule con mayor facilidad por el sistema; además contiene componentes con alimentación mejorada en todo el gabinete. El diseño de hardware optimizado complementa las sofisticadas capacidades de administración de alimentación integradas en el Chassis Management Controller (CMC), los suministros de energía y el iDRAC para mejorar aún más la eficiencia de alimentación y permitir el control total del 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 PowerEdge M1000e consume alimentación y distribuye la carga por todas las unidades de suministro de energía internas que están activas. El sistema puede producir hasta 16685 vatios de alimentación de entrada, que se asignan a los módulos del servidor y a la infraestructura del gabinete.

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.

Puede controlar la administración de la alimentación desde **Consola para medir, mitigar y administrar la alimentación (PM3)**. Cuando PM3 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 del suministro de energía (DPSE)
- Operación a 110 VCA. Esto solo se admite en unidades de suministro de energía de CA.

PM3 administra lo siguiente:

- Alimentación del servidor
- Prioridad de los servidores
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

NOTA: La entrega real de alimentación se basa en la configuración y en la carga de trabajo.

Puede utilizar la interfaz web 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.

Enlaces relacionados

Políticas de redundancia

Puede ejecutar la siguiente operación de control de alimentación para chasis, servidores y módulos de E/S.

Políticas de redundancia

La política de redundancia es un conjunto configurable de propiedades que determina la forma en que el CMC administra la alimentación al chasis. Las siguientes políticas de redundancia son configurables con conexión dinámica de unidad de suministro de energía o sin ella:

- Redundancia de cuadrícula
- Redundancia del suministro de energía
- No redundancia

Política de redundancia de la red eléctrica

El objetivo de la política de redundancia de la red eléctrica es permitir que un sistema de gabinete modular pueda funcionar de un modo que le permita tolerar las fallas de alimentación. Es posible que estas fallas se originen en la red eléctrica de entrada, el cableado o el suministro o bien, en la propia unidad de suministro de energía.

Cuando se configura un sistema para tener redundancia de la red eléctrica, las unidades de suministro de energía se dividen en redes eléctricas: las unidades de las ranuras 1, 2 y 3 se encuentran en la primera red eléctrica, en tanto que las unidades de las ranuras 4, 5 y 6 se encuentran en la segunda red eléctrica. El 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 las unidades de suministro de energía individuales.

NOTA: La redundancia de la red eléctrica ofrece una operación transparente del servidor aunque existan fallas de una red eléctrica entera. En consecuencia, la alimentación máxima está disponible para mantener la redundancia de la red eléctrica cuando las capacidades de las dos redes sean 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, debe existir al menos una unidad de suministro de energía en cada red eléctrica. Es posible definir configuraciones adicionales con cada combinación que tenga al menos una unidad de suministro de energía en cada red eléctrica. Sin embargo, para que el máximo nivel de energía esté disponible para su uso, la energía total de las unidades de suministro de energía 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. En la siguiente figura se muestran dos unidades de suministro de energía 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.

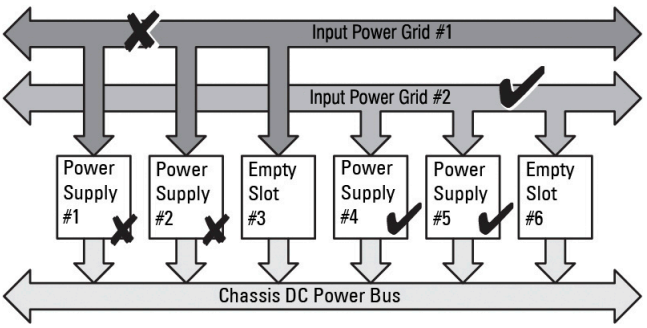


Ilustración 5. Unidades de suministro de energía por cada red eléctrica y una falla de alimentación en la red eléctrica 1

En el caso de que falle una sola unidad de suministro de energía en esta configuración, las unidades de suministro de energía restantes de la red eléctrica que presenta la falla se marcarán con el estado En línea. En este estado, cualquiera de las unidades de suministro de energía restantes puede fallar sin interrumpir el funcionamiento del sistema. Si una unidad de suministro de energía falla, la condición del chasis aparece como no crítica. Si la red eléctrica más pequeña no puede admitir todas las asignaciones de alimentación del chasis, el estado de redundancia de la red eléctrica aparecerá como **Sin redundancia** y la condición del chasis aparecerá como **Crítica**.

Política de redundancia de suministro de energía

La política de redundancia de suministro de energía es útil cuando las redes de energía redundante no están disponibles, pero es posible que desee estar protegido contra una falla de una única unidad de suministro de energía que deje fuera de servicio a los servidores en un gabinete modular. La unidad de suministro de energía de mayor capacidad se mantiene en reserva en línea para este propósito. Esto forma un grupo de redundancia de suministro de energía. 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 CA, cuando se selecciona la redundancia de suministro de energía el CMC no requiere que las unidades de suministro de energía estén presentes en ninguna posición específica de las ranuras de las unidades de suministro de energía.

NOTA: La conexión dinámica del suministro de energía (DPSE) permite poner en espera las unidades de suministro de energía. El estado En espera indica una condición física durante la cual no se suministra alimentación desde la unidad de suministro de energía. Al activar DPSE, las unidades de suministro de energía adicionales pueden ponerse en modo de espera para aumentar la eficiencia y ahorrar energía.

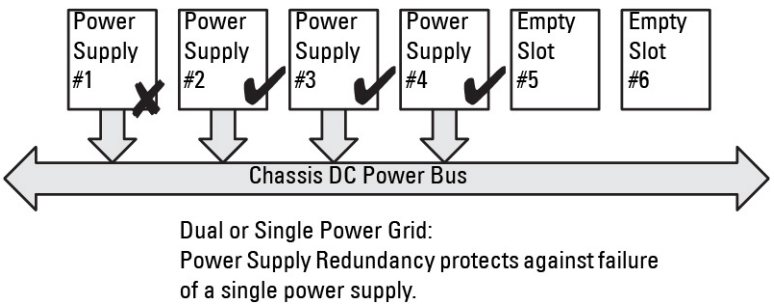


Ilustración 6. Redundancia de suministro de energía: total de 4 unidades de suministro de energía con la falla de una unidad

Sin política de redundancia

El modo sin redundancia es el valor predeterminado de fábrica para la configuración de 3 unidades de suministro de energía e indica que el chasis no tiene redundancia de alimentación configurada. En esta configuración, el estado de

redundancia general del chasis indicará siempre Sin redundancia. En la figura a continuación se muestra el modo sin redundancia que es el valor predeterminado de fábrica para la configuración de 3 unidades de suministro de energía.

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 unidades de suministro de energía del chasis aparecerán **En línea** si la DPSE está desactivada durante el modo **Sin redundancia**. Cuando se activa la DPSE, todas las unidades de suministro de energía activas en el chasis aparecen en la lista con el estado **En línea** y las unidades adicionales pueden pasar al estado **En espera** para mejorar la eficiencia energética del sistema.

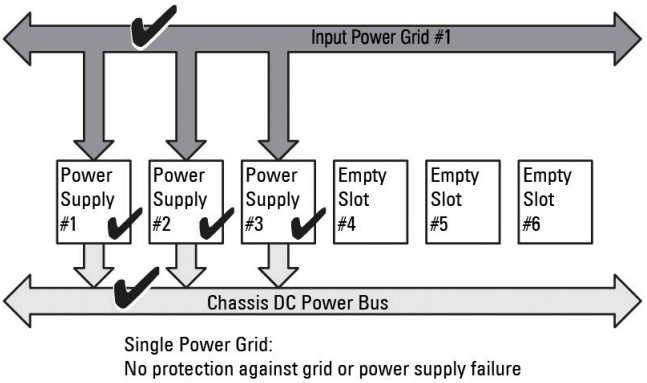


Ilustración 7. Sin redundancia con tres unidades de suministro de energía en el chasis

Una falla en una unidad de suministro de energía hace que las demás unidades de suministro de energía salgan del modo En espera, según sea necesario, para cubrir las asignaciones de energía del chasis. Si existen cuatro unidades de suministro de energía y solo se requieren tres, en caso de que una falle, la cuarta unidad se pone en línea. Un chasis puede tener las 6 unidades de suministro de energía en línea.

Al activar DPSE, las unidades de suministro de energía adicionales pueden ponerse en modo de espera para aumentar la eficiencia y ahorrar energía. Para obtener más información, consulte Default Redundancy Configuration (Configuración predeterminada de redundancia).

Conexión dinámica de suministros de energía

El modo Conexión dinámica del suministro de energía (DPSE) está desactivado de manera predeterminada. Para ahorrar energía, DPSE optimiza la eficiencia energética proporcionada por las unidades de suministro de energía al chasis. Esto también aumenta la vida útil de las unidades de suministro de energía y reduce la generación de calor.

El CMC supervisa la asignación de alimentación total del gabinete y mueve los al estado En espera. Al mover 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 una gran eficiencia energética, con una cantidad óptima de unidades de suministro de energía en línea. Las unidades de suministro de energía que no se necesitan se colocan en el modo de espera.
- El modo **Redundancia de unidad de suministro de energía** con DPSE también proporciona eficiencia energética. Por lo menos dos suministros están en línea: una unidad alimenta la configuración y la otra proporciona redundancia en caso de falla de la unidad de suministro de energía. El modo Redundancia de unidad de

suministro de energía ofrece protección contra cualquier falla de unidad de suministro de energía, pero no ofrece protección en caso de una pérdida de la red 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 DPSE proporciona la más baja eficiencia ya que las seis fuentes están activas 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 espera**. En una configuración de seis unidades de suministro de energía, algunas unidades se pondrán **En espera** y no se utilizarán para mejorar la eficiencia energética. La eliminación o falla de una unidad de suministro de energía en línea en esta configuración ocasiona que una unidad en modo **En espera** pase al modo **En línea**. Sin embargo, las unidades de suministro de energía 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 de **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 con **Redundancia de suministro de energía**, el gabinete siempre mantiene una unidad de suministro de energía adicional encendida y marcada como **En línea** además de las unidades necesarias para alimentar el gabinete. La utilización de alimentación se supervisa y hasta cuatro unidades de suministro de energía pueden ponerse En espera dependiendo de la carga general del sistema. En una configuración de seis unidades de suministro de energía, por lo menos dos unidades de suministro de energía se encuentran siempre encendidas.

  Puesto que un gabinete en configuración de **Redundancia de suministro de energía** siempre tiene una unidad de suministro de energía adicional conectada, el gabinete puede tolerar la pérdida de una unidad de suministro de energía en línea. Aún así, el gabinete puede tener suficiente energía para los módulos de servidor instalados. La pérdida de la unidad de suministro de energía en línea hará que una unidad en espera se ponga en línea. La falla simultánea de varias unidades de suministro de energía puede ocasionar la pérdida de corriente en algunos módulos de servidor mientras que las unidades de suministro de energía en espera se encienden.
- En la configuración 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 permite, las PSU se mueven al estado **En espera**. El estado **En línea** de las PSU en una red eléctrica replica el de la otra red. En consecuencia, el gabinete puede soportar la pérdida de energía de toda la 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 unidades de suministro de energía se activen y salgan del estado **En espera**. Esto mantiene la configuración duplicada necesaria para 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 35. 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, las seis unidades están activas. Las tres unidades de suministro de energía de la izquierda deben estar conectadas a una red de entrada, mientras que las tres unidades de suministro de energía de la derecha deben estar conectadas a otra red de energía.

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 un conjunto equilibrado de unidades de suministro de energía (al menos una unidad en cada red eléctrica). Si esta condición no se cumple, la redundancia de la red eléctrica no será posible.

Redundancia del suministro de energía

Cuando se activa la redundancia de suministro de energía, una de las unidades de suministro de energía del chasis se mantiene como repuesto, lo cual garantiza que la falla de una de las unidades no ocasione que se apaguen los servidores o el chasis. El modo de redundancia de suministro de energía requiere hasta cuatro unidades de suministro de energía. Si existen unidades de suministro de energía adicionales, serán utilizadas para mejorar la eficiencia energética del sistema cuando la DPSE esté activada. Las fallas posteriores a una pérdida de redundancia pueden provocar que los servidores del chasis se apaguen.

Sin 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 cuando DPSE se activa por requisitos del chasis. Cuando se está en este modo, la falla de una sola unidad de suministro de energía 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.

La siguiente figura muestra un chasis con una configuración de seis unidades de suministro de energía. Las unidades se numeran de 1 a 6 a partir del lado izquierdo del gabinete.

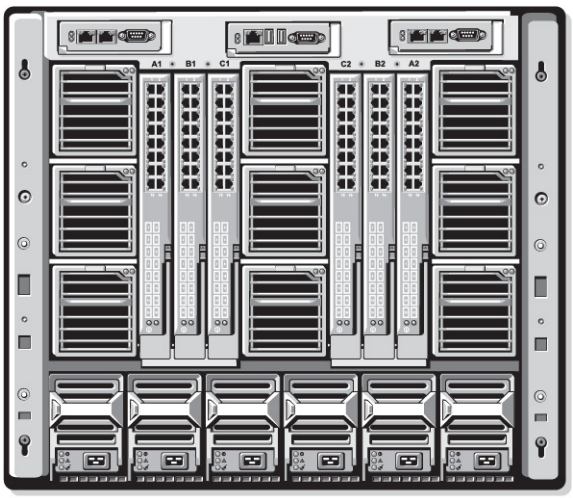


Ilustración 8. Configuración de chasis con seis unidades de suministro de energía

El CMC mantiene un presupuesto de alimentación para el gabinete que reserva la potencia necesaria para todos los servidores y componentes instalados.

El CMC asigna alimentación a la infraestructura del CMC y a los servidores del chasis. La infraestructura del CMC consta de los componentes dentro del chasis, por ejemplo, ventiladores, módulos de E/S o iKVM (si está presente). El chasis puede contener hasta 16 servidores que se comunican con el chasis mediante el iDRAC. Para obtener más información, consulte *iDRAC7 User's Guide (Guía del usuario de iDRAC7)* ubicada en **support.dell.com/manuals**.

El iDRAC proporciona al CMC el requisito de envolvente de potencia antes de encender el servidor. La envolvente de potencia consiste en los requisitos de alimentación máxima y mínima para mantener el servidor en funcionamiento. El cálculo inicial del iDRAC se basa en la comprensión inicial de los componentes en el servidor. Después de iniciar el funcionamiento y de detectar otros componentes, el iDRAC puede aumentar o reducir sus requisitos de alimentación iniciales.

Cuando se enciende un servidor en un gabinete, el software del iDRAC vuelve a calcular los requisitos de alimentación y solicita el cambio correspondiente en la envolvente de potencia.

El 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 iDRAC del servidor supervisa continuamente el consumo de alimentación real. Según los requerimientos reales de alimentación, la envolvente de potencia del iDRAC puede ser modificada con el paso del tiempo. 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 permite especificar un *Límite de alimentación de entrada del sistema* para garantizar que el consumo global de corriente alterna del chasis permanezca por debajo de un umbral determinado. El CMC primero garantiza que haya suficiente alimentación disponible para que funcionen los ventiladores, los módulos de E/S, el iKVM (si está presente) y el propio CMC. Esta asignación de energía se denomina *Alimentación de entrada asignada a la infraestructura de chasis*. Después de la infraestructura del chasis, los servidores de un gabinete se encienden. Todo intento por definir un valor de *Límite de alimentación de entrada del sistema* inferior al consumo real fracasará.

Si para el presupuesto total de alimentación es necesario permanecer por debajo del valor de *Límite de alimentación de entrada del sistema*, el CMC asignará a los servidores un valor menor que la alimentación máxima solicitada. Se asigna

alimentación a los servidores en función de la configuración de *Prioridad del servidor*, en la que 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 de acuerdo con la *Capacidad de alimentación máxima de entrada del sistema* y el valor de *Límite de alimentación de entrada del sistema* que el usuario haya configurado.

Los cambios de configuración, como un servidor adicional en el chasis, pueden requerir un aumento en el *Límite de alimentación de entrada del sistema*. Las necesidades de alimentación de un gabinete modular aumentan también al cambiar las condiciones térmicas que requieren que los ventiladores funcionen a mayor velocidad, lo cual ocasiona un consumo adicional de alimentación. 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 a la controladora de administración encendida.

Los servidores adicionales pueden encenderse en un gabinete modular solamente si hay suficiente alimentación disponible. El valor del *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

El CMC permite que los usuarios establezcan una prioridad de alimentación para cada una de las 16 ranuras de servidores de un gabinete. Los valores de prioridad son de 1 (la más alta) a 9 (la más baja). Estos valores se asignan a las ranuras del chasis y todo servidor insertado en esa ranura heredará la prioridad de la ranura. El CMC utiliza la prioridad de ranura para administrar alimentación con preferencia para los servidores de más alta prioridad en el gabinete.

Según el valor predeterminado de prioridad de ranura de servidor, la alimentación se distribuye por igual a todas las ranuras. El cambio de prioridades de ranura permite a los administradores priorizar a qué servidores se les dará preferencia al asignar alimentación. Si los módulos de servidor más importantes se dejan con la prioridad de ranura predeterminada de 1 y los módulos de servidor menos críticos se cambian a un valor más bajo de prioridad de 2 o un número mayor, primero se dará alimentación a los módulos de servidor de prioridad 1. Estos servidores de prioridad más alta obtendrían su asignación máxima de alimentación, mientras que a los servidores de prioridad más baja no se les asignaría suficiente alimentación para funcionar a su máximo rendimiento o no se encenderían en absoluto. Esto depende del valor mínimo en el que se establezca el límite de alimentación de entrada del sistema y los requisitos de alimentación del servidor.

Si un administrador enciende manualmente los módulos de servidor de baja prioridad antes que los de prioridad más alta, los módulos de servidor de prioridad baja serán los primeros módulos a los que se les disminuya su asignación de alimentación a su valor mínimo, a fin de abastecer a los servidores de mayor prioridad. Por lo tanto, cuando se agota la alimentación disponible para la asignación, el CMC retira alimentación de los servidores de prioridad inferior o igual hasta que alcanzan el nivel mínimo de alimentación.

NOTA: A los módulos de E/S, los ventiladores e iKVM (si está presente) se les asigna la más alta prioridad. El CMC recupera alimentación solo de los dispositivos de menor prioridad para satisfacer las necesidades de alimentación de módulos o servidores de más alta 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. Si traslada el servidor a una nueva ranura, debe reconfigurar la prioridad para la ubicación de la nueva ranura.

NOTA: Para realizar acciones de administración de 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, siendo 1 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 <número de ranura>
<nivel de prioridad>
```

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

El 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 mediante la interfaz web del CMC, vaya a **Descripción general del chasis** y haga clic en **Alimentación → Supervisión de alimentación**. La página Supervisión de alimentación muestra la condición de la alimentación, el estado de la alimentación del sistema, y estadísticas de alimentación y de energía en tiempo real. Para obtener más información, consulte la sección *CMC Online Help (Ayuda en línea del CMC)*.

NOTA: También puede ver el estado de redundancia de alimentación en la opción Suministros de energía en **Árbol del sistema → ficha 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 de presupuesto de alimentación mediante la interfaz web del CMC, en el árbol del sistema vaya a **Descripción general del chasis** y haga clic en **Alimentación** → **Estado de presupuesto**. La página **Estado de presupuesto de alimentación** muestra la configuración de la política de alimentación del sistema, los detalles del presupuesto de alimentación, el presupuesto asignado para los módulos del servidor y los detalles del suministro de energía del chasis. Para obtener más información, consulte *CMC Online Help (Ayuda en línea del 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** de *RACADM Command Line Reference Guide for iDRAC6 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC6 y CMC)*.

Estado de redundancia y condición general de la alimentación

El estado de redundancia es un factor determinante de la condición general de la alimentación. Cuando se establece la política de redundancia de alimentación, por ejemplo, en Redundancia de la red eléctrica, y el estado de redundancia indica que el sistema funciona con redundancia, la condición general de la alimentación normalmente será **En buen estado**. Sin embargo, si no se satisfacen las condiciones para operar con redundancia de la red eléctrica, el estado de redundancia será **En mal estado** y la condición general de la alimentación será **Crítica**. Esto se debe a que el sistema no puede funcionar de acuerdo con la política de redundancia configurada.

NOTA: El CMC no realiza una comprobación previa de estas condiciones cuando la política de redundancia se cambia a Redundancia de la red eléctrica o se cambia de esta última a otra. Por lo tanto, configurar la política de redundancia podría ocasionar inmediatamente una pérdida de redundancia o una condición de recuperación.

Enlaces relacionados

Falla de la unidad de suministro de energía con política de redundancia Degradada o Sin redundancia
Retiro de unidades de suministro de energía con política de redundancia Degradada o Sin redundancia.
Política de conexión de servidores nuevos
Cambios de suministro de energía y política de redundancia en el registro de sucesos del sistema

Falla de la unidad de suministro de energía con política de redundancia Degradada o Sin redundancia

El CMC reduce la alimentación a los servidores cuando se produce un caso de alimentación insuficiente, por ejemplo, la falla de una unidad de suministro de energía. Después de reducir la alimentación a los servidores, el CMC vuelve a evaluar las necesidades de alimentación del chasis. Si aún no se cumplen los requisitos de alimentación, el CMC apagará los servidores de menor prioridad.

La alimentación a los servidores de mayor prioridad se restablece gradualmente, en tanto que las necesidades de alimentación se ajustan al presupuesto de alimentación. Para establecer la política de redundancia, consulte Configuring Power Budget and Redundancy (Configuración de la redundancia y el presupuesto de alimentación).

Retiro de unidades de suministro de energía con política de redundancia Degradada o Sin redundancia.

Es posible que el CMC comience a conservar energía cuando se quita una unidad de suministro de energía o se quita el cable de CA de una unidad de suministro de energía. El CMC reduce la alimentación de los servidores con menor prioridad hasta que el consumo de energía pueda ser cubierto por las unidades de suministro de energía restantes en el chasis. Si quita más de una unidad de suministro de energía, el CMC volverá a evaluar las necesidades de alimentación al quitar la segunda unidad a fin de determinar la respuesta del firmware. Si aún no se cumplen los requisitos de alimentación, es posible que el CMC apague los servidores de menor prioridad.

Límites

- El CMC no admite el apagado *automatizado* de un servidor con menor prioridad para permitir el encendido de un servidor con mayor prioridad; sin embargo, se pueden realizar apagados iniciados por el usuario.
- Los cambios en la política de redundancia de las unidades de suministro de energía están limitados por el número de unidades de suministro de energía en el chasis. Se puede seleccionar cualquiera de los tres valores de configuración de la redundancia de las unidades de suministro de energía que se citan en Configuración de redundancia predeterminada.

Política de conexión de servidores nuevos

Si un servidor nuevo que está encendido supera la alimentación disponible para el chasis, es posible que el CMC disminuya la alimentación hacia los servidores de menor prioridad. Esto permite que el nuevo servidor reciba más alimentación. Esto sucede en los siguientes casos:

- 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 hacer funcionar el chasis y todos los servidores con alimentación máxima, incluso el nuevo, es el requisito de alimentación para el peor de los casos. Si esa alimentación está disponible, el límite de suministro de energía que se asignará a los servidores no será inferior al 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 36. 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	Permitido No permitido

Se cuenta con alimentación para el peor de los casos	Respuesta del CMC	Encendido del servidor
	• La alimentación requerida para el nuevo servidor no está disponible	

Si una unidad de suministro de energía falla, se produce un estado no crítico y se genera un suceso de falla de unidad de suministro de energía. Al desmontar una unidad de suministro de energía se genera un suceso de desmontaje de una unidad de suministro de energía.

Si uno de los sucesos ocasiona una pérdida de redundancia, en función de las asignaciones de alimentación, se genera un suceso de *pérdida de redundancia*.

Si la capacidad de alimentación posterior o la capacidad de alimentación del usuario es mayor que las asignaciones de los servidores, el rendimiento de los servidores se verá degradado o, en el peor de los casos, los servidores pueden llegar a apagarse. Ambas condiciones se dan en orden de prioridad inverso, es decir, los servidores de menor prioridad se apagan primero.

En la siguiente tabla se describe la respuesta del firmware ante el apagado o el desmontaje de una unidad de suministro de energía conforme se aplica a diversas configuraciones de redundancia de las unidades de suministro de energía.

Tabla 37. 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 unidades de suministro de energía en modo de espera (si existen) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el desmontaje de una unidad de suministro de energía.
Redundancia del suministro de energía	Activado	El CMC informa al usuario que hay pérdida de redundancia de suministro de energía. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el desmontaje de una unidad de suministro de energía.
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 registran anotaciones en el registro de sucesos del sistema (SEL) son inserción y extracción de suministros de energía, inserción y extracción de entrada de suministros de energía, y declaración y retiro de declaración de salida de suministros de energía.

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

Tabla 38. 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>).
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 registran anotaciones en el SEL son la pérdida de redundancia y la recuperación de redundancia para el gabinete modular que está configurado para una política de alimentación de **Redundancia de la red eléctrica** o para una política de **Redundancia de suministro de energía**. La lista a continuación muestra las anotaciones del SEL relacionadas con los cambios en la política de alimentación de redundancia.

Tabla 39. 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

Es posible 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), que utiliza seis unidades de suministro de energía. 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 del servidor sobre redundancia de alimentación
- Activar conexión dinámica del suministro 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

Enlaces relacionados

Conservación de la energía y presupuesto de alimentación
Modo de conservación máxima de energía
Reducción de la alimentación del servidor para mantener el presupuesto de alimentación
Operación de unidades de suministro de energía de 110 V
Rendimiento del sistema sobre redundancia de alimentación
Registro remoto
Administración de la alimentación externa
Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web del CMC
Configuración de la redundancia y el presupuesto de alimentación mediante RACADM

Conservación de la energía y presupuesto de alimentación

El 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, el CMC reduce la alimentación a los servidores en orden de prioridad inverso. Esto permite que haya energía para los servidores de mayor prioridad y otros módulos del chasis.

Si todas o varias ranuras del chasis están configuradas con el mismo nivel de prioridad, el CMC disminuye la alimentación a medida que aumenta el número de ranuras. Por ejemplo, si los servidores en las ranuras 1 y 2 tienen el mismo nivel de prioridad, la alimentación para el servidor en la ranura 1 se reduce antes que la del servidor en la ranura 2.

NOTA: Puede asignar un nivel de prioridad a cada uno de los servidores en el chasis asignándole un número del 1 al 9 a cada uno. El nivel de prioridad 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 máximo equivalente al de cualquier grupo de tres unidades de suministro de energía que sea el más débil. Si intenta establecer un valor de presupuesto de alimentación de CA que exceda el valor de *Límite de alimentación de entrada del sistema*, el CMC mostrará un mensaje de falla. El presupuesto de alimentación se limita a 16685 vatios.

Modo de conservación máxima de energía

El CMC realiza una conservación máxima de la 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 de asignación de energía del servidor se rechazan. En este modo, el rendimiento de los servidores encendidos puede degradarse. Los servidores adicionales no pueden encenderse, independientemente de la prioridad del servidor.

El sistema se restablece al rendimiento óptimo cuando se desactiva el modo de conservación máxima.

Reducción de la alimentación del servidor para mantener el presupuesto de alimentación

El CMC reduce la asignación de alimentación a los servidores de menor prioridad cuando se necesita energía adicional para mantener el consumo de alimentación del sistema dentro del valor de *Límite de alimentación de entrada del sistema*. Por ejemplo, mediante la administración y la supervisión de alimentación 297 cuando se conecta un nuevo servidor, el CMC podría 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 a los servidores de menor prioridad la cantidad de energía aún no es suficiente, el 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 admiten la operación con una entrada de 110 V de CA. Esta entrada puede superar el valor permitido para el circuito. Si alguna de las unidades de suministro de energía está conectada a 110 V de CA, el usuario deberá configurar el CMC para que el gabinete funcione normalmente. Si no se configura de esta manera y se detectan unidades de suministro de energía de 110 V, todas las solicitudes posteriores de asignación de alimentación del servidor se rechazarán. En este caso, los servidores adicionales no podrán encenderse, independientemente de su prioridad. Puede configurar el CMC para utilizar unidades de suministro de energía de 110 V por medio de la interfaz web o el comando 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 confirmó 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 admiten operaciones combinadas de 110 V y 220 V. Si el CMC detecta ambos voltajes, se selecciona uno de los dos y los suministros de energía conectados al otro voltaje se apagan y se marcan como fallidos.

Rendimiento del sistema sobre redundancia de alimentación

Cuando está activada, esta opción favorece el rendimiento y el encendido del servidor ante el mantenimiento de la redundancia de alimentación. Cuando está desactivada, el sistema favorece la redundancia de alimentación ante el rendimiento del servidor. Cuando está desactivada, si los 298 suministros de energía de administración y supervisión del chasis no proporcionan suficiente alimentación tanto para redundancia como para el rendimiento total, si se quiere conservar redundancia, es posible que deba ocurrir lo siguiente en algunos servidores:

- No se les otorgue suficiente alimentación para un rendimiento completo
- No se enciendan

Registro remoto

Se puede informar sobre el consumo de alimentación a un servidor syslog remoto. Es posible registrar información sobre el consumo total del chasis, el consumo de alimentación mínimo, máximo y medio en un período de recopilación.

Para obtener más información sobre la manera de activar esta función y configurar el intervalo de recopilación y registro, consulte la sección Ejecución de operaciones de control de alimentación.

Administración de la alimentación externa

De forma opcional, la administración de alimentación del CMC se puede controlar mediante la consola para medir, mitigar y administrar la alimentación (PM3). Para obtener más información, consulte *PM3 User's Guide* (Guía del usuario de PM3).

Si está activada la administración de la alimentación externa, la PM3 administra lo siguiente:

- Alimentación del servidor en servidores de 12ª generación
- Prioridad del servidor en servidores de 12ª generación
- 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

Entonces, la PM3 administra la priorización y la alimentación de los servidores blade de 12ª generación del chasis con el presupuesto disponible tras 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 la alimentación externa.

Una vez que se haya activado el modo de administración de la alimentación basada en servidor, el chasis estará preparado para la administración de la PM3. La prioridad de todos los servidores de 12ª generación está definida en 1 (Alta). La PM3 administra las prioridades y la alimentación de los servidores directamente. La PM3 controla las asignaciones de alimentación de servidores compatibles, por lo que el CMC ya no controla el modo de conservación máxima de energía y esta selección está desactivada.

Si se activa el modo de conservación máxima de energía, el CMC establece la capacidad de alimentación de entrada del sistema en el máximo que admite el chasis. El CMC no permite que la alimentación supere la capacidad máxima. Sin embargo, la PM3 administra todos los demás límites de capacidad de alimentación.

Si la administración de la alimentación de la PM3 está desactivada, el CMC vuelve a los valores de prioridad de los servidores configurados antes de que se activase la administración externa.

NOTA: Cuando la administración de la PM3 está desactivada, el CMC no vuelve a la configuración anterior de la alimentación máxima del chasis. Consulte el **registro del CMC** para conocer la configuración anterior y restaurar el valor manualmente.

Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web del CMC

NOTA: Para realizar acciones de administración de 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 cualquiera de las siguientes propiedades según corresponda. Para obtener información acerca de cada uno de los campos, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
   - Activar alimentación basada en servidor
   - Límite de alimentación de entrada del sistema
   - Política de redundancia
   - Rendimiento del sistema sobre redundancia de alimentación
   - Activar conexión dinámica del suministro de energía
   - Desactivar botón de encendido del chasis
   - Permitir operación a 110 VCA
   - 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 el 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 <*valor*> 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 establece la política de redundancia en 1:
     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
     ```
   - Para establecer el valor del presupuesto de alimentación, escriba:
     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap <value>
     ```
     donde <*valor*> es un número entre 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 presupuesto máximo de la alimentación 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 <*valor*> es 0 Usuarios locales (desactivar), 1 (activar). El valor predeterminado es 0.

     Por ejemplo, el siguiente comando desactiva el acoplamiento dinámico de unidades de suministro de energía:
     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable 0
     ```
     .

- Para activar el modo de consumo máximo de alimentación, escriba:

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

- Para restaurar el funcionamiento normal, escriba:

  ```
  racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode
  0
  ```

- 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 de syslog remotos se hayan configurado previamente. El registro en uno o más hosts de syslog 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 de **configuración del syslog remoto** en *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)*, disponible en **dell.com/support/manuals**.

- Para activar la administración de la alimentación remota con la Consola para medir, mitigar y administrar la alimentación (PM3), escriba lo siguiente:

  ```
  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 *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

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.

Enlaces relacionados

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 el 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 **Apply (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 <*acción*> es `powerup`, `powerdown`, `powercycle`, `nongraceshutdown` o `reset`.

Ejecución de operaciones de control de alimentación en un servidor

Es posible realizar acciones de administración de alimentación de forma remota para varios servidores a la vez o un servidor individual en el chasis.

NOTA: Para realizar acciones de administración de 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 **Apply (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 **Apply (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 *<módulo>* especifica el servidor por su número de ranura (servidor 1 a 16) en el chasis y *<acción>* 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><acción>
```

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.

Recopilación de información de configuración, registros y estado del chasis mediante RACDUMP

El subcomando `racdump` permite utilizar un solo comando para obtener información completa sobre el estado del chasis, datos de estado de configuración y registros históricos de sucesos.

El subcomando `racdump` muestra la siguiente información:

- Información general del sistema/RAC
- Información del 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 y agrega los siguientes comandos de RACADM. Para obtener más información sobre racdump, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC)*.

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 MIB (Base de información de administración) SNMP

El archivo MIB SNMP del CMC define los indicadores, sucesos y tipos de chasis. El CMC permite descargar el archivo MIB a través de 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 configuró la **Política de redundancia de alimentación** con la opción **Redundancia de CA** y apareció un suceso de Redundancia de suministro de energía perdida.

- **Solución A**: esta configuración requiere al menos un suministro de energía en el lado 1 (las tres ranuras de la izquierda) y un suministro de energía en el lado 2 (las tres ranuras de la derecha) que estén 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 **redundancia de CA**. (Para garantizar una completa operación de redundancia de CA, asegúrese de que haya una configuración completa de seis unidades de suministro de energía).
- **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 **redundancia de CA** se pierde cuando una de las redes 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 funciona como se espera. Si no se soluciona el error, comuníquese con el departamento de atención al cliente de Dell para reemplazar el suministro de energía.
  - **Solución B:** revise que la unidad de suministro de energía esté conectada al mismo voltaje que las otras unidades. Si el CMC detecta que una unidad de suministro de energía está funcionando con un voltaje distinto, la unidad se apaga y se marca como fallida.
- **Problema:** 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 del suministro de energía no se puede admitir por completo con las unidades de suministro de energía presentes en este gabinete. Para verificar si es así, utilice la interfaz web a fin de desactivar la **conexión dinámica del suministro de energía** y luego volver a activarla. Si la conexión del suministro de energía dinámica 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 los circuitos 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 el valor de conservación máxima de energía. Si esta opción está establecida, los servidores estarán autorizados a 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 CMC 1.2 y posteriores tienen administración dinámica de alimentación de ventiladores que reduce brevemente la asignación de alimentación a los servidores si el gabinete opera cerca del límite máximo de alimentación configurado por el usuario. Hace que se asigne alimentación a los ventiladores mediante la reducción del rendimiento del servidor para mantener el consumo de alimentación de entrada por debajo del **Límite de alimentación de entrada del sistema**.

- **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 en la red de CA, aun cuando el chasis estaba operando en la configuración de **Redundancia de CA** 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 en que ocurre la falla en la red de CA. La política de **Redundancia de CA** requiere que se conecten los tres suministros de energía de la izquierda a una red de CA, y los tres suministros de energía de la derecha a otra red de CA. Si se conectan dos unidades de suministro de energía, por ejemplo, PSU3 y PSU4, a las redes de CA equivocadas, una falla en la red de CA ocasionará la pérdida de alimentación en los servidores de menor prioridad.
- **Problema:** los servidores de menor prioridad perdieron alimentación después de una falla en una unidad de suministro de energía.
  - **Solución:** este comportamiento es normal si la política de alimentación de gabinete se configuró como **Sin redundancia**. Para evitar que una falla de alimentación futura ocasione que se apaguen los servidores, asegúrese de que el chasis tenga como mínimo cuatro suministros de energía y se configure de manera que la política de **Redundancia de suministro de energía** evite que la falla en una unidad de suministro de energía afecte la operación del servidor.
- **Problema:** el rendimiento general del servidor disminuye cuando aumenta la temperatura ambiente en el centro de datos.
  - **Solución:** esto puede ocurrir si el **Límite de alimentación de entrada del sistema** se configuró con un valor que provoca que una necesidad de alimentación mayor de los ventiladores se tenga que compensar con una reducción de alimentación para los servidores. El usuario puede aumentar el **Límite de alimentación de entrada del sistema** a un valor mayor de modo que se permita la asignación de alimentación adicional a los ventiladores sin afectar el rendimiento del servidor.

Solución de problemas de alertas

Use el registro del CMC y el registro de rastreo para solucionar problemas con los alertas del CMC. El éxito o la falla de cada intento de entrega de las capturas de SNMP o de correo electrónico se anota en el registro del CMC. En el registro de rastreo se incluye información adicional que describe el error específico. Sin embargo, dado que SNMP no confirma la entrega de capturas, utilice un analizador de red o una herramienta como snmputil de Microsoft para rastrear los paquetes en el sistema administrado.

Enlaces relacionados

Configuración del CMC para enviar alertas

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.

Enlaces relacionados

Visualización del registro de hardware
Visualización del registro del CMC

Visualización del registro de hardware

El CMC genera un registro de sucesos de hardware que ocurren en el chasis. Para ver el registro de hardware, utilice la interfaz web y RACADM remoto.

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

NOTA: Puede configurar el CMC para enviar capturas SNMP o un correo electrónico cuando ocurran sucesos específicos. Para obtener información sobre la configuración del CMC para enviar alertas, consulte Configuring CMC to Send Alerts (Configuración del 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
```

Enlaces relacionados

Visualización de los registros de sucesos

Visualización de los registros de hardware mediante la interfaz web del CMC

Es posible ver, guardar y eliminar el registro de hardware. También es posible ordenar las entradas del registro según la gravedad, fecha y hora o la descripción al hacer clic en el encabezado de la columna. Los clics posteriores que realice en los encabezados de la columna revertirán este orden.

Para ver los registros de hardware mediante la interfaz web del CMC, en el árbol del sistema, vaya a **Descripción del chasis** y haga clic en **Registros → Registro de hardware**. Aparecerá la página **Registro de hardware**. Para guardar una copia del registro de hardware en la estación o la red administrada, haga clic en **Guardar registro** y especifique una ubicación para un archivo de texto del registro.

NOTA: Dado que el registro se guarda como archivo de texto, no se mostrarán las imágenes gráficas usadas para indicar la gravedad en la interfaz de usuario. En el archivo de texto, la gravedad se indica con las palabras Aceptar, Informativo, Desconocido, Advertencia y Grave. Las entradas de fecha y hora aparecen en orden ascendente. Si <SYSTEM BOOT> aparece en la columna **Fecha/hora**, significa que el suceso se produjo durante un apagado o inicio de cualquiera de los módulos, cuando no hay disponible ninguna fecha ni hora.

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

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

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

Enlaces relacionados

Visualización de los registros de sucesos

Visualización de los registros del CMC mediante la interfaz web

Puede ver, guardar y borrar el registro del CMC. Asimismo, puede ordenar las anotaciones en el registro en función del origen, la fecha/hora o la descripción; para ello, haga clic en el encabezado de la columna. Para invertir el orden, continúe haciendo clic en los encabezados.

Para ver el registro del CMC a través de la interfaz web, en el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Registros → Registro del CMC**. Se mostrará la página **Registro del 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
```

Para borrar el registro de hardware, escriba:

```
racadm clrraclog
```

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

Es posible restablecer el CMC activo, restablecer el iDRAC sin reiniciar el sistema operativo o volver a colocar virtualmente los servidores de modo tal que se comporten como si se los hubiese quitado y vuelto a insertar. Si el chasis tiene un CMC en espera, el restablecimiento del CMC activo produce una protección contra fallas y el CMC en espera se vuelve 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 el CMC activo, en la sección **Estado del CMC**, haga clic en **Restablecimiento/Protección contra fallas de CMC**. Si un CMC en espera está presente y un chasis es totalmente redundante, se produce una protección contra fallas que provoca que el CMC en espera pase a estar activo.
3. Para restablecer el iDRAC solamente, sin reiniciar el sistema operativo, en la sección **Restablecer servidor**, haga clic en **Restablecimiento del iDRAC** en el menú desplegable **Restablecer** para los servidores cuyo iDRAC desea restablecer y luego haga clic en **Aplicar selecciones**. De esta manera, se restablecen los iDRAC correspondientes a 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 por medio de RACADM, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC)*.

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 **Guardar**. Sobrescriba la ruta del archivo predeterminada (opcional) y haga clic en **Aceptar** para guardar el archivo.

NOTA: El nombre de archivo predeterminado de la copia de seguridad contiene la etiqueta de servicio del chasis. Este archivo de copia de seguridad puede utilizarse posteriormente para restaurar los valores y certificados de este chasis en particular.

Para restaurar la configuración del chasis, haga clic en **Elegir archivo**, especifique el archivo de copia de seguridad y haga clic en **Restaurar**.

NOTA: CMC no se reinicia al restaurar la configuración; sin embargo, es posible que se requiera algo de tiempo para que los servicios del CMC asimilen los cambios o la nueva configuración. Una vez que el proceso se complete correctamente, se cerrarán todas las sesiones actuales.

Solución de errores de protocolo de hora de red (NTP)

Después de configurar el CMC de modo que el reloj esté sincronizado con un servidor de hora remota en la red, pueden transcurrir de 2 a 3 minutos hasta que se refleje un cambio en la fecha y hora. Si transcurrido este tiempo no se produce ningún cambio, es posible que sea necesario solucionar algún problema. El CMC no puede sincronizar el reloj por alguna de 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 del CMC. Este registro contiene mensajes de error para las fallas relacionadas con NTP. Si el CMC no puede sincronizarse con los servidores NTP remotos configurados, la hora del CMC se sincronizará con el reloj del sistema local y el registro de rastreo incluirá una anotación 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. El resultado de este comando contiene estadísticas de NTP detalladas que pueden resultar útiles para la depuración del 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 sus consecuencias, ya que el valor predeterminado debe ser lo suficientemente alto para que funcione con la mayoría de los servidores NTP.

Para modificar el parámetro, escriba el comando siguiente:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

Después de realizar el cambio, desactive el NTP, espere entre 5 y 10 segundos y active el NTP nuevamente:

NOTA: NTP puede tardar 3 minutos más para sincronizarse nuevamente.

Para desactivar el NTP, escriba:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

Para activar el NTP, escriba:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

Si los servidores NTP se configuraron correctamente y esta anotación está presente en el registro de rastreo, se confirmará que el CMC no puede sincronizarse con ninguno de los servidores NTP configurados.

Si no está configurada la dirección IP del servidor NTP, posiblemente verá una anotación del registro de rastreo similar a:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address
1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Si se configuró un valor del servidor NTP con un nombre de host no válido, posiblemente verá una anotación del registro de rastreo similar a:

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21
14:34:27 cmc ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

Para obtener información acerca de cómo se introduce el comando `gettracelog` a fin de revisar el registro de rastreo mediante la interfaz web del CMC, consulte Using Diagnostic Console (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 está parpadeando, indica un suceso crítico pero de rutina, por ejemplo una carga de firmware, durante el cual la unidad no es operativa. Este estado no indica una falla.
- Los LED que parpadean en color ámbar en un módulo indican una falla en ese módulo.
- Los LED que parpadean en color azul pueden ser configurados por el usuario y utilizados para identificación. Consulte la sección Downloading SNMP Management Information Base (MIB) File (Descarga del archivo MIB [Base de información de administración] SNMP).

Tabla 40. Colores y patrones de parpadeo de los LED

Componente	Color de LED, patrón de parpadeo	Status (Estado)
CMC	Verde, encendido permanentemente	No se enciendan
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado

Componente	Color de LED, patrón de parpadeo	Status (Estado)
	Azul, encendido permanentemente	Activo
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Modo de espera
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

Componente	Color de LED, patrón de parpadeo	Status (Estado)
	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
	Ámbar, parpadeante	Falla del ventilador; tacómetro fuera de rango
	Ámbar, apagado	No se utiliza
la 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 la energía. Si no está encendido:
  - Verifique que haya corriente alterna presente en al menos un suministro de energía.
  - Verifique que la tarjeta del CMC esté colocada correctamente. Puede liberar o tirar de la palanca de expulsión, extraer el CMC y volver a instalarlo asegurándose de que la placa esté insertada completamente y el seguro cierre correctamente.
- LED inferior: el indicador LED inferior es de varios colores. Cuando el CMC está activo y en funcionamiento, y no hay ningún problema, el LED inferior es azul. Si es de color ámbar, se ha detectado una falla. La falla podría producirse por cualquiera de los siguientes tres sucesos:

- Una falla del núcleo. En este caso, se debe reemplazar la placa del CMC.
- Una falla de autoprueba. En este caso, se debe reemplazar la placa del CMC.
- Una imagen dañada. En este caso, cargue la imagen de firmware del CMC para recuperar el CMC.

NOTA: Un inicio o restablecimiento normal del CMC demora un poco más de un minuto para iniciar su sistema operativo completamente y quedar disponible para el inicio de sesión. El indicador LED azul está activado en el CMC activo. En una configuración redundante con dos CMC, solo el LED verde superior está activado en el 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 elija (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, habrá disponible información adicional. La petición indica el número de ranura del CMC y el tipo de falla.

   Para ver el motivo de la falla y la sintaxis para 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 habrá componentes utilizables en el CMC. El CMC está dañado 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

El CMC entra en el modo de recuperación cuando no es posible realizar un inicio normal del sistema operativo del CMC. En el modo de recuperación, hay un pequeño subconjunto de comandos disponible 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 e inicia el sistema operativo del CMC una vez que se completa.

Cuando escribe recover y luego presiona <Intro> en la petición recuperación, aparece el motivo de la recuperación y los subcomandos disponibles. Un ejemplo de secuencia de recuperación podría ser:

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
recover ping 192.168.0.100 recover fwupdate -g -a 192.168.0.100
```

NOTA: Conecte el cable de red al conector RJ45 del extremo izquierdo.

NOTA: En el modo de recuperación, no puede enviar comandos ping al CMC normalmente porque no hay ningún apilamiento de red activo. El comando `recover ping <IP del servidor TFTP>` 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 del CMC permite depurar los sistemas de alerta y de red del CMC. Es posible obtener acceso al registro de rastreo a través de la interfaz web del CMC o de RACADM. Consulte la sección del comando `gettracelog` en *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos de RACADM para iDRAC7 y CMC).

El registro de rastreo da seguimiento a la siguiente información:

- DHCP: rastrea los paquetes que se envían a un servidor DHCP y que se reciben de él.
- DDNS: rastrea solicitudes y respuestas de actualización de DNS dinámico.
- Cambios de configuración en las interfaces de red.

El registro de rastreo también puede contener códigos de error específicos del firmware del CMC que están relacionados con el firmware interno del CMC, no con el sistema operativo del sistema administrado.

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. La garantía no cubre los daños ocasionados por reparaciones que Dell no haya autorizado. Lea y siga las instrucciones de seguridad que se incluyen con el producto.

Para realizar acciones de administración, se requiere un usuario con privilegios de **Administrador**. El software del 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 a través del puente PASSWORD_RSET en la placa del CMC.

La placa del CMC tiene un conector de restablecimiento de contraseña con dos clavijas 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 activarán y tomarán los valores predeterminados de `nombre de usuario: root` y `contraseña: calvin`. La cuenta del administrador se restablecerá independientemente de que se haya eliminado la cuenta o se haya cambiado la contraseña.

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

Para realizar acciones de administración, se requiere un usuario con privilegios de **Administrador**. Si se olvida la contraseña de la cuenta del administrador, es posible restablecerla a través del puente PASSWORD_RST en la placa del 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:

```
nombre de usuario: root
contraseña: 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 seguro de liberación del CMC en la palanca y aleje la palanca del panel frontal del módulo. Deslice el módulo CMC hasta extraerlo del gabinete.

   NOTA: Las descargas electroestáticas pueden causar daños al CMC. En determinadas condiciones, las cargas electroestáticas pueden acumularse en el cuerpo o en algún objeto y luego descargarse en el CMC. Para evitar daños ocasionados por descargas electroestáticas, tome las precauciones necesarias para descargar toda electricidad estática de su cuerpo antes de manipular u obtener acceso al 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 del CMC.

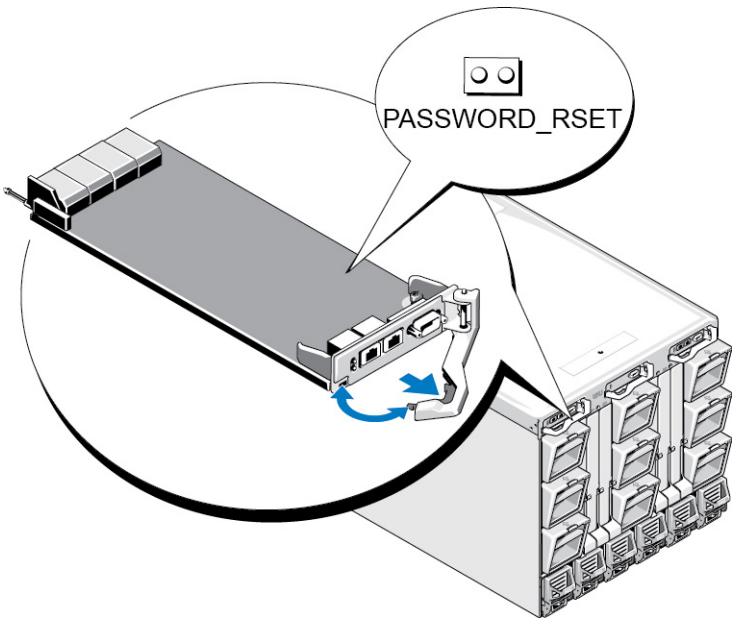


Ilustración 9. Ubicación del puente de restablecimiento de contraseña

Tabla 41. Opciones del puente de contraseña del CMC

PASSWORD_RST		(predeterminada)	La función de restablecimiento de contraseña está desactivada.
			La función de restablecimiento de contraseña está activada.

3. Deslice el módulo CMC hacia adentro del 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 CMC con puente es el único CMC, espere a que finalice el reinicio. Si hay un CMC redundante en el chasis, inicie un cambio para activar el módulo CMC con puente. En la interfaz web, en el árbol del sistema, vaya a

Descripción general del chasis y haga clic en **Alimentación → Control**, seleccione **Restablecer el CMC (reinicio mediante sistema operativo)** y haga clic en **Aplicar**.

El CMC cederá automáticamente sus funciones al módulo redundante y este último se convertirá en el módulo activo.

5. Inicie sesión en el CMC activo con el nombre de usuario root y la contraseña calvin predeterminados de administrador, y restaure la configuración pertinente de la cuenta de usuario. Las cuentas y contraseñas existentes no están desactivadas y 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 seguro de liberación del CMC en la palanca y aleje la palanca del panel frontal del módulo. Deslice el módulo CMC hasta extraerlo del gabinete.
   b) Quite el puente de dos clavijas y vuelva a colocar el tapón del puente.
   c) Deslice el módulo CMC hacia adentro del gabinete. Vuelva a conectar los cables que se desconectaron. Repita el paso 4 para que el módulo CMC sin puente se convierta en el CMC activo.

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 los menús, los iconos, los mensajes y las imágenes.

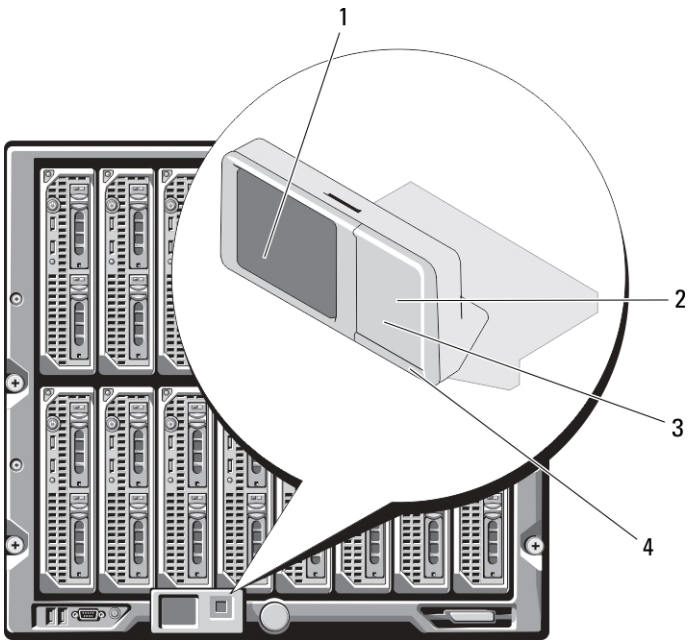


Ilustración 10. Pantalla LCD

1	Pantalla LCD	2	Botón de selección ("check")
3	Botones de desplazamiento (4)	4	LED indicador de estado

Enlaces relacionados

- Navegación de la pantalla LCD
- Diagnóstico
- Solución de problemas del hardware de LCD
- Mensajes de la pantalla LCD del panel frontal
- Mensajes de error de la pantalla LCD
- Información de estado del servidor y del módulo de LCD

Navegación de la pantalla LCD

El lado derecho del panel LCD tiene cinco botones: cuatro botones de flecha (arriba, abajo, izquierda y derecha) y un botón central.

- *Para desplazarse por las pantallas, use los botones de flecha derecha (siguiente) e izquierda (anterior). Mientras se usa el panel, es posible regresar a una pantalla anterior en cualquier momento.*
- *Para desplazarse a través de las opciones en una pantalla, utilice los botones de flecha hacia abajo y arriba.*
- *Para seleccionar y guardar un elemento en una pantalla y avanzar a la siguiente pantalla, utilice el botón central.*

Los botones de flecha hacia arriba, abajo, izquierda y derecha cambian los objetos o los iconos del menú seleccionados en la pantalla. El objeto 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 42. 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.

Enlaces relacionados

Menú principal
Menú de configuración de LCD
Pantalla de configuración de idioma
Pantalla predeterminada
Pantalla de estado gráfico del servidor
Pantalla de estado gráfico del módulo
Pantalla del menú Gabinete
Pantalla de estado del módulo
Pantalla Estado del gabinete
Pantalla Resumen de IP

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 seleccione el icono **Atrás** si desea regresar al menú **Principal**.

Para activar la opción seleccionada, presione el botón central.

Pantalla de configuración de idioma

La pantalla **Configuración de idioma** permite seleccionar el idioma usado para los mensajes del panel LCD. El idioma actualmente activo está resaltado con un fondo celeste.

1. Use los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia la derecha para resaltar el idioma deseado.
2. Presione el botón central.
   Aparecerá el icono **Aceptar** resaltado.
3. Para confirmar el cambio, presione el botón central.
   Aparecerá el menú **Configuración de LCD**.

Pantalla predeterminada

La opción **Pantalla predeterminada** permite cambiar la pantalla que el panel LCD muestra cuando no hay ninguna actividad en el panel. La pantalla predeterminada de fábrica es **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 **Estado gráfico del servidor** muestra iconos para cada servidor instalado en el chasis e indica el estado de condición general de cada servidor. La condición del servidor se indica mediante el color del icono de 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 deseado y presione el botón central. Aparecerá la pantalla **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 **Estado gráfico del módulo** muestra todos los módulos que están instalados en la parte posterior del chasis y ofrece un resumen con la información de condición de cada módulo. La condición del módulo se indica con 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 las flechas hacia arriba, abajo, derecha e izquierda para seleccionar el módulo indicado y presione el botón central. Se mostrará la pantalla **Estado del módulo**.

Para regresar a **Menú principal,** use los botones de flecha para seleccionar el icono Atrás y luego presione el botón central. Se mostrará **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 correspondiente (seleccione el icono **Atrás** para regresar a **Menú principal**) y presione el botón central. Se mostrará la pantalla seleccionada.

Pantalla de estado del módulo

La pantalla **Estado del módulo** muestra información y mensajes de error de cada módulo. Para ver los mensajes que pueden aparecer en esta pantalla, consulte las secciones LCD Module and Server Status Information (Información de estado del servidor y módulo de LCD) y LCD Error Messages (Mensajes de error de la pantalla LCD).

Use las flechas hacia arriba y hacia abajo para moverse por los mensajes. Use las flechas hacia la izquierda y hacia 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 **Estado del gabinete** muestra la información y los mensajes de error del gabinete. Para ver los mensajes que pueden aparecer en esta pantalla, consulte LCD Error Messages (Mensajes de error de LCD). Use las teclas de flecha hacia arriba y abajo para desplazarse 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 flechas hacia arriba y hacia abajo para desplazarse por la lista. Use las flechas hacia la izquierda y hacia la derecha para desplazarse por los mensajes seleccionados que no caben en la pantalla.

Use los botones de flechas hacia arriba y hacia abajo para seleccionar el icono **Atrás** y presione el botón central para regresar al menú **Gabinete**.

Diagnóstico

El panel LCD permite diagnosticar problemas en cualquier servidor o módulo del chasis. Si hay un problema o se produjo una falla en el chasis, en cualquier servidor o en cualquier módulo del chasis, el indicador de estado del panel LCD parpadea en color ámbar. En Menú principal, un icono con fondo ámbar aparece junto al elemento del menú (Servidor o Gabinete) que conduce al servidor o módulo fallido.

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 errores del servidor, use la interfaz web o la interfaz de línea de comandos del iDRAC para borrar el Registro de sucesos del sistema (SEL). En los errores del chasis, use la interfaz web o la interfaz de línea de comandos del 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.

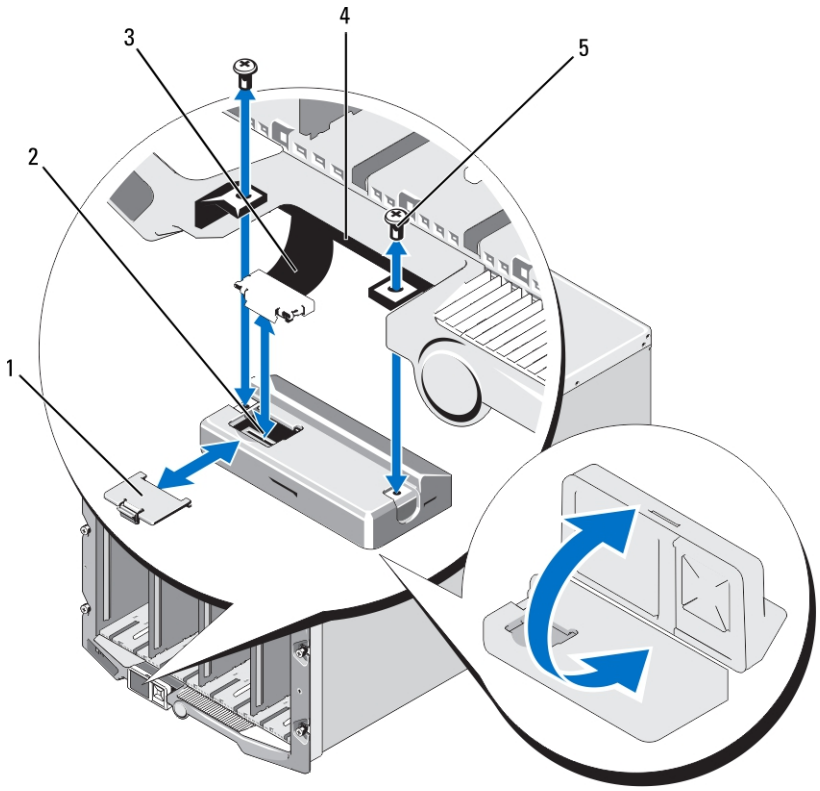


Ilustración 11. Extracción e instalación del módulo LCD

1	Cubierta de cables	2	Módulo LCD
3	Cable plano	4	Bisagras (2)
5	Tornillos (2)		

Tabla 43. Elementos de solución de problemas del hardware de LCD

Síntoma	Problema	Acción de recuperación
Aparece un mensaje de alerta de pantalla `CMC no responde` y el LED está 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.
Aparece un mensaje de alerta de pantalla `CMC no responde` y el LED de color ámbar oscuro está 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 interfaz gráfica de usuario o los comandos de RACADM. Busque el mensaje que dice: `Can not communicate with LCD controller (No es posible comunicarse con la controladora LCD).` 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 interfaz gráfica de usuario o los comandos de RACADM. Busque el mensaje que dice: • `El cable del módulo LCD no está conectado o no está conectado correctamente.` • `El cable del panel de control no está conectado o no está conectado correctamente.` Vuelva a colocar los cables.
Mensaje de pantalla LCD `No CMC Found (No se encontró CMC).`	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.

La tabla en la sección de errores muestra los mensajes de error y de advertencia que aparecen en las diferentes pantallas LCD y la causa posible de cada mensaje. El texto entre comillas angulares (< >) indica que el texto puede variar.

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 44. 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	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	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 45. 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.
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.	El CMC ya no es redundante. Esto sucede cuando se elimina el 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	El registro está lleno.	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 46. 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 47. 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 48. 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 49. Pantallas de estado de la unidad de suministro de energía

Gravedad	Mensaje	Causa
Crítico	Se ha producido un error en la fuente de alimentación <número>.	Se produjo una falla en la unidad de suministro de energía.
Crítico	Se ha perdido la entrada de corriente de la fuente de alimentación <número>.	Pérdida de energía de CA o cable de CA sin conectar.
Aviso	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 50. 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.

Gravedad	Mensaje	Causa
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	Se ha producido un error interno [IERR] en la CPU <número>.	Falla de la CPU.
Crítico	Se ha producido un evento de control térmico [exceso de temperatura] en la CPU <número>.	La CPU se sobrecalentó.
Crítico	No está admitida la configuración de la CPU <número>.	Tipo de procesador o ubicación incorrectos.
Crítico	Falta la CPU <número>.	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	Se ha extraído la unidad <number>.	La unidad de almacenamiento fue eliminada.
Crítico	Falla detectada en la unidad <número>.	Se produjo una falla en la unidad de almacenamiento.

Gravedad	Mensaje	Causa
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.
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	El registro está lleno.	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	Se ha detectado un error de paridad de PCI en un componente de la ranura <número>.	Se detectó un error de paridad en el bus PCI.

Gravedad	Mensaje	Causa
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	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 ha detectado 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.
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	La ROM de opción de la tarjeta intermedia <número> 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 51. Estado del CMC

Elemento	Descripción
Ejemplo: CMC1, CMC2	Nombre o ubicación.
Sin errores	Si no existen errores, aparecerá el mensaje “Sin errores”; de lo contrario aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos por las advertencias.
Versión del firmware	Solo se muestra en un CMC activo. Muestra el mensaje “En espera” para el CMC que está 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.

Tabla 52. Estado del chasis o del gabinete

Elemento	Descripción
Nombre definido por el usuario	Ejemplo: “Sistema de bastidores Dell”. Puede configurar esta opción a través de la interfaz de línea de comandos (CLI) o la interfaz web del CMC.
Mensajes de error	Si no existen errores, aparecerá el mensaje “Sin errores”; de lo contrario aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos por 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 53. 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 54. 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 "Sin errores"; de lo contrario aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos por las advertencias.
Status (Estado)	Desconectado, Conectado o En espera.
Potencia máxima	Potencia máxima que la unidad de suministro de energía puede proporcionar al sistema.

Tabla 55. Estado del módulo de E/S

Elemento	Descripción
Nombre/Ubicación	Ejemplo: IOM A1, IOM B1, y así sucesivamente.
Mensajes de error	Si no existen errores, aparecerá el mensaje "Sin errores"; de lo contrario aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos por las advertencias. Para obtener más información, consulte LCD Error Messages (Mensajes de error del LCD).
Status (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 los módulos de E/S están encendidos. En el tipo de módulo de E/S de paso el valor es cero.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.

Tabla 56. Estado de iKVM

Elemento	Descripción
Name (Nombre)	iKVM.
Sin errores	Si no existen errores, aparecerá el mensaje “Sin errores”; de lo contrario aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos por las advertencias. Para obtener más información, consulte LCD Error Messages (Mensajes de error del LCD).
Status (Estado)	Encendido o Apagado.
Modelo/fabricante	Descripción del modelo de iKVM.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.
Número de parte	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 57. Estado del servidor

Elemento	Descripción
Ejemplo: Servidor 1, Servidor 2, etc.	Nombre/Ubicación.
Sin errores	Si no existen errores, aparecerá el mensaje “Sin errores”; de lo contrario aparecerá una lista de mensajes de error. Los errores críticos aparecerán primero, seguidos por las advertencias. Para obtener más información, consulte LCD Error Messages (Mensajes de error del LCD).
Nombre de ranura	Nombre de ranura del chasis. Por ejemplo, RANURA-01. **NOTA:** Puede configurar esta tabla a través de la CLI o la interfaz web del CMC.
Name (Nombre)	Nombre del servidor, que el usuario puede establecer mediante Dell OpenManage. El nombre se muestra únicamente si el iDRAC completó el inicio y si el servidor admite esta función; en caso contrario, se muestran los mensajes de inicio de iDRAC.
Número de modelo	Se muestra si el iDRAC completó el inicio.
Etiqueta de servicio	Se muestra si el iDRAC completó el inicio.
Versión del BIOS	Versión del firmware del BIOS del servidor.
Último código de la POST	Muestra la cadena de mensajes del último código de la POST del BIOS del servidor.
Versión del firmware del iDRAC	Se muestra si el iDRAC completó el inicio.

	NOTA: La versión del iDRAC 1.01 se muestra como 1.1. No hay versión 1.10 del iDRAC.
IP4 <activado, desactivado>	Muestra el estado actual activado del IPv4.
Dirección IP4: <dirección, adquiriendo>	Solo se muestra si IPv4 está activado.
IP6 <activado, desactivado>	Solo se muestra si el iDRAC admite IPv6. Muestra el estado actual activado del IPv6.
Dirección local IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
Dirección global IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
FlexAddress activado en la red Fabric	Solo se muestra si la función está instalada. Enumera las redes Fabric activadas para dicho servidor (es decir, A, B, C).

La información de la tabla se actualiza de forma dinámica. Si el servidor no admite esta función, la siguiente información no aparecerá; 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 el iDRAC completó el inicio. Para obtener más información sobre esta función, consulte *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC)* 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

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 y nombres incorrectos. Ejemplo: `ERROR: <message>`

Use el subcomando `help` de RACADM para mostrar la sintaxis correcta y la información de uso.

Mensajes de error relacionados con el CMC: problemas donde el CMC no puede realizar una acción. También puede decir "racadm command failed" (Falló el comando racadm).

Escriba `racadm gettracelog` para obtener información sobre la depuración de errores.

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.

Se mostrará el mensaje de error "No se encontró" al utilizar los comandos `$ logout` y `$ quit`.

Los comandos logout y quit no se admiten en la interfaz de RACADM del CMC.

Administración 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 del CMC predeterminado para garantizar la seguridad de la red en las funciones de la interfaz web y de RACADM remoto. Cuando se utiliza este certificado, el explorador web muestra una advertencia de seguridad cuando el certificado predeterminado se emite para un certificado predeterminado del CMC que 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 que haya sido emitido para la dirección IP del CMC. Al generar la solicitud de firma de certificado (CSR) que se utilizará para emitir el certificado,

asegúrese de que el nombre común (CN) de la CSR tenga la misma dirección IP que el CMC (por ejemplo, 192.168.0.120) o el mismo 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 **Registrar el CMC** en la opción **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 del RACADM remoto y la interfaz tarden algunos minutos en estar disponibles después de restablecer el servidor web del CMC. El servidor web del CMC se restablece después de que ocurre lo siguiente:

   - 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** (incluso cuando un comando `config -f <config file>` la cambia).
   - Se utiliza `racresetcfg` o se restablece una copia de seguridad de la configuración del chasis.
   - Se restablece el 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 del 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 del CMC predeterminado para garantizar la seguridad de la red en las funciones de la interfaz web y de RACADM remoto. Este certificado no es emitido por una autoridad de certificados confiable. Para solucionar este problema de seguridad, cargue un certificado de servidor del CMC que haya sido emitido por una autoridad de certificados confiable (por ejemplo, Thawte o Verisign). Para obtener más información acerca de cómo emitir certificados, consulte Obtaining Certificates (Obtención de certificados).

   ¿Por qué se muestra el mensaje siguiente por motivos desconocidos?

   Remote Access: SNMP Authentication Failure

   Como parte del descubrimiento, IT Assistant intenta verificar los nombres de comunidad **Get** y **Set** del dispositivo. En IT Assistant, usted tiene el nombre de **comunidad get = public** y el **nombre de comunidad set = private**. De manera predeterminada, el nombre de comunidad para el agente CMC es "public". Cuando IT Assistant envía una solicitud de comunidad Set, el agente CMC genera el error de autentificación SNMP porque solo acepta solicitudes de **comunidad = public**.

   Cambie el nombre de comunidad del CMC desde RACADM. Para ver el nombre de comunidad del CMC, use el siguiente comando:

   ```
   racadm getconfig -g cfgOobSnmp
   ```

   Para establecer el nombre de comunidad del CMC, utilice el siguiente comando:

   ```
   racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
   ```

Para evitar que se generen capturas de autentificación SNMP, debe utilizar nombres de comunidad que acepte el agente. Como el CMC solo permite un nombre de comunidad, debe introducir el mismo nombre de comunidad Get y Set para la configuración de descubrimiento de IT Assistant.

Active Directory

¿Admite Active Directory el inicio de sesión en el CMC en varios árboles?

Sí. El algoritmo de consulta de Active Directory del CMC admite varios árboles en un solo bosque.

¿El inicio de sesión en el CMC mediante Active Directory funciona en el modo mixto (es decir, los controladores de dominio del bosque ejecutan diferentes sistemas operativos, como Microsoft Windows 2000 o Windows Server 2003)?

Sí. En el modo mixto, todos los objetos utilizados por el proceso de consulta del CMC (entre el usuario, el objeto del dispositivo del RAC y el objeto de asociación) tienen que estar en el mismo dominio.

El complemento Usuarios y equipos de Active Directory extendido por Dell verifica el modo y limita a los usuarios a fin de crear objetos en varios dominios si se encuentra en modo mixto.

¿El uso del CMC con Active Directory admite varios entornos de dominio?

Sí. El nivel de la función del bosque de dominios debe estar en el modo Nativo o en el modo Windows 2003. Asimismo, los grupos entre el objeto de asociación, los objetos de usuario de RAC y los objetos de dispositivo de RAC (incluido el objeto de asociación) deben estar en grupos universales.

¿Estos objetos extendidos por Dell (objeto de asociación Dell, dispositivo de RAC de Dell y objeto de privilegio Dell) pueden estar en dominios diferentes?

El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento Usuarios y equipos de Active Directory extendido por Dell permite crear estos dos objetos solamente en el mismo dominio. Otros objetos pueden estar en diferentes dominios.

¿Existe alguna restricción para la configuración del controlador de dominio de SSL?

Sí. Todos los certificados SSL para los servidores Active Directory que se encuentran en el bosque deben estar firmados mediante el mismo certificado con firma de la autoridad de certificados raíz, pues el CMC solo permite cargar un certificado SSL firmado por una autoridad de certificados de confianza.

La interfaz web no se inicia una vez que se creó y se cargó un nuevo certificado RAC.

Si se utilizan los servicios de certificados de Microsoft para generar el certificado RAC, es posible que se haya utilizado la opción Certificado de usuario en lugar de Certificado web durante la creación del certificado.

Para solucionar el problema, genere una CSR, cree un certificado web nuevo utilizando los servicios de certificados de Microsoft y cárguelo mediante los siguientes comandos de RACADM:

```
racadm sslcsrgen [-g] [-f {nombre de archivo}]
racadm sslcertupload -t 1 -f {cert_SSL_de_web}
```

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 = YYYYYYY
```

An entry is added to the CMC log that states:

cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis ID='XXXXXXXX'

¿Qué sucede si se quita la tarjeta de función y se instala una tarjeta que no sea de FlexAddress?

No se activa ni se modifica la tarjeta. El CMC ignora la tarjeta. En este caso, el comando **$racadm featurecard -s** muestra el siguiente mensaje:

No feature card inserted

ERROR: can't open file

Si se reprograma la etiqueta de servicio del chasis, ¿qué sucede si hay una tarjeta de función vinculada a ese chasis?

- Si la tarjeta de función original está presente en el CMC activo en ese u otro chasis, 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

  (Esta tarjeta de función se activó con otro chasis. Debe quitarse para acceder a la función FlexAddress).

  Current Chassis Service Tag = XXXXXXXX (Etiqueta de servicio del chasis actual = XXXXXXXX)

  Feature Card Chassis Service Tag = YYYYYYYY (Etiqueta de servicio del chasis de la tarjeta de función = YYYYYYYY)

  The original feature card is no longer eligible for deactivation on that or any other chassis, unless Dell Service re-programs the original chassis service tag back into a chassis, and CMC that has the original feature card is made active on that chassis (La tarjeta de función original ya no está disponible para su desactivación en ese u otro chasis, a menos que Dell Service reprograme la etiqueta de servicio del chasis original 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 y refleja 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 un mensaje de error. La tarjeta de función en el CMC activo está activa e instalada en el chasis. El CMC ignora la segunda tarjeta.

¿La tarjeta SD tiene un dispositivo de protección contra escritura?

Sí. Antes de instalar la tarjeta SD en el módulo de CMC, verifique que el seguro de protección contra escritura esté desbloqueado. La función FlexAddress no podrá activarse si la tarjeta SD está protegida contra escritura. En este caso, el comando **$racadm feature -s** muestra el siguiente mensaje:

No features active on the chassis. ERROR: read only file system

¿Qué sucede si no hay una tarjeta SD en el módulo CMC activo?

El comando **$racadm featurecard -s** muestra este mensaje:

No feature card inserted.

¿Qué le sucede a la función FlexAddress si el BIOS del servidor se actualiza de la versión 1.xx a la versión 2.xx?

Se debe apagar el módulo del servidor para poder usarlo con FlexAddress. Una vez completada la actualización del BIOS del servidor, el módulo del servidor no recibirá direcciones asignadas por el chasis hasta que se haya activado el ciclo de encendido del servidor.

¿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 del CMC de este chasis se actualice a la versión 1.10 o superior, la función FlexAddress se reactivará reinsertando la tarjeta de función original (si fuera necesario), restableciendo el 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 del CMC en espera no se actualiza a la versión 1.10 o 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 el CMC al momento de desactivar FlexAddress. Para recuperar el uso de la tarjeta, insértela de nuevo en un CMC del chasis con el que esté vinculada, reinstale FlexAddress y luego desactive FlexAddress nuevamente.

La tarjeta SD está correctamente instalada y se realizaron todas las actualizaciones de firmware o software. La función FlexAddress está activa, pero la pantalla de implementación del servidor no muestra las opciones para implementarla. ¿Cuál es el problema?

Este es un problema de almacenamiento en caché del explorador; cierre el explorador 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 en forma predeterminada todas las ranuras y redes Fabric.

NOTA: Se recomienda especialmente apagar el chasis antes de ejecutar el comando `racresetcfg` de RACADM.

Después de desactivar únicamente la función FlexAddressPlus (dejando activada FlexAddress), ¿por qué falla el comando racadm setflexaddr en el CMC (aún activo)?

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 del CMC") aparece en el monitor conectado al panel frontal. ¿Por qué?

El CMC desactivó la conexión del panel frontal. Active el panel frontal desde la interfaz web del CMC o con un comando de 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 iKVM Connection Precedences (Prioridades de conexión 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 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 en el iKVM**, por lo que este debe reprogramarse. Para solucionar el problema, siga las instrucciones para actualizar el firmware del iKVM.
- **El módulo iKVM está reprogramando la interfaz de consola del CMC.** En este caso, la consola de CMC no se encuentra disponible por el momento y está representada por un punto de color amarillo en la interfaz OSCAR. Este proceso puede tardar 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 de iKVM, los conectores ACI y del panel posterior están desactivados.

Para activar la conexión del puerto ACI, primero debe desactivar el acceso al panel frontal o quitar el monitor que tiene conectado. 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 → Configuración**, desactive la opción **Video/USB del panel frontal activado** y haga clic en 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 OSCAR, la conexión del CMC de Dell muestra una cruz (X) de color rojo y no es posible conectarse al CMC. ¿Por qué?

Existen dos causas posibles:

- **Dell CMC console fue desactivada.** En este caso, para activarla puede utilizar la interfaz web del CMC o un comando de RACADM.
- **El CMC no está disponible porque se está inicializando, se está conmutando al CMC en espera o se está reprogramando.** En este caso, espere hasta que el 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 seleccionarse 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 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 **Actualizar** para ver si la dirección IP está correctamente configurada 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.

En este momento, solo los exploradores Mozilla Firefox e Internet Explorer admiten SSO. Verifique que la configuración del explorador sea correcta. Para obtener más información, consulte la sección Configuración del explorador para el inicio de sesión único.

Si los exploradores están configurados correctamente, ambos deben permitirle iniciar sesión sin introducir el nombre y la contraseña. Use el nombre de dominio completo (FQDN) para el CMC. Por ejemplo, **miCMC.Dominio.ext/**, en la barra de direcciones del explorador. El explorador lo redirigirá a **https** (modo seguro) y le permitirá iniciar sesión en el CMC. Tanto **http** como **https** son válidos para los exploradores. Si guarda la URL como favorito, no deberá introducir texto después de la última barra en el ejemplo. Si aún no puede iniciar sesión con SSO, consulte la sección Configuración del CMC para inicio de sesión único o inicio de sesión mediante tarjeta inteligente 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.

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. El CMC se encuentra preinstalado en el chasis; por lo tanto, no es necesario realizar ninguna instalación. Es posible instalar un segundo CMC para que se ejecute como componente en espera para el CMC activo.

   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 del CMC principal, el CMC en espera asume el rol del CMC 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 del iDRAC. No afecta a la conectividad externa entre los servidores y los módulos de E/S.
3. Para actualizar el firmware del iDRAC o Lifecycle Controller sin inactividad en el chasis, realice la actualización con el servicio de Lifecycle Controller. Para obtener más información sobre la actualización de firmware de componentes de servidores con Lifecycle Controller, consulte la sección Actualización de firmware de los componentes del servidor.

   NOTA: Al actualizar cualquier otro componente, como tarjetas mezzanine, controladoras NDC y el BIOS, se producirá una inactividad de los servidores.