

Firmware de Dell Chassis
Management Controller
Versión 4.0

Guía del usuario



Notas y precauciones



NOTA: una NOTA proporciona información importante que le ayudará a utilizar mejor el equipo.



PRECAUCIÓN: un mensaje de PRECAUCIÓN indica la posibilidad de que se produzcan daños en el hardware o haya pérdida de datos si no se siguen las instrucciones.

La información contenida en esta publicación puede modificarse sin previo aviso.
© 2010-2011 Dell Inc. Todos los derechos reservados.

Queda estrictamente prohibida la reproducción de este material en cualquier forma sin la autorización por escrito de Dell Inc. Marcas comerciales utilizadas en este texto: Dell™, el logotipo de DELL, FlexAddress™, OpenManage™, PowerEdge™ y PowerConnect™ son marcas comerciales de Dell Inc. Microsoft®, Active Directory®, Internet Explorer®, Windows®, Windows Server® y Windows Vista® son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y/o en otros países. Red Hat® y Red Hat Enterprise Linux® son marcas comerciales registradas de Red Hat, Inc. en los Estados Unidos y en otros países. Novell® es una marca comercial registrada y SUSE™ es una marca comercial de Novell Inc. en los Estados Unidos y en otros países. Intel® es una marca comercial registrada de Intel Corporation. UNIX® es una marca comercial registrada de The Open Group en los Estados Unidos y en otros países. Avocent® es una marca comercial de Avocent Corporation. OSCAR® es una marca comercial registrada de Avocent Corporation o sus filiales.

Copyright 1998-2006 The OpenLDAP Foundation. Todos los derechos reservados. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, solo según lo autoriza la licencia pública de OpenLDAP. Hay una copia de esta licencia disponible en el archivo LICENSE en el directorio principal de la distribución o, como alternativa, en <http://www.OpenLDAP.org/license.html>. OpenLDAP es una marca comercial registrada de OpenLDAP Foundation. Hay archivos individuales y/o paquetes recibidos en contribuciones que pueden ser propiedad intelectual de terceros y están sujetos a restricciones adicionales. Este trabajo se deriva de la distribución LDAP v3.3 de la Universidad de Michigan. Este trabajo también contiene materiales que provienen de fuentes públicas. La información sobre OpenLDAP se puede obtener en <http://www.openldap.org/>. Porciones de Copyright 1998-2004 Kurt D. Zeilenga. Porciones de Copyright 1998-2004 Net Boolean Incorporated. Porciones de Copyright 2001-2004 IBM Corporation. Todos los derechos reservados. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, solo según lo autoriza la licencia pública de OpenLDAP. Porciones de Copyright 1999-2003 Howard Y.H. Chu. Porciones de Copyright 1999-2003 Symas Corporation. Porciones de Copyright 1998-2003 Hallvard B. Furuseth. Todos los derechos reservados. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, siempre y cuando se conserve este aviso. Los nombres de los titulares de la propiedad intelectual no se deben usar para promocionar o promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece "tal cual" sin garantías expresas o implícitas. Porciones de Copyright (c) 1992-1996 Regentes de la Universidad de Michigan. Todos los derechos reservados. Se permite la redistribución y uso en formatos binario y original siempre y cuando se conserve este aviso y se conceda el crédito correspondiente a la Universidad de Michigan en Ann Arbor. El nombre de la universidad no se debe usar para promocionar ni promover productos derivados de este software sin previo permiso específico por escrito. Este software se ofrece "tal cual" sin garantías expresas o implícitas.

En esta publicación se pueden usar otras marcas y nombres comerciales para referirse a las entidades que los poseen o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

Contenido

1	Descripción general	21
	Novedades de esta versión	22
	Funciones de administración del CMC	23
	Funciones de seguridad	25
	Descripción general del chasis	26
	Especificaciones del hardware	27
	Puertos TCP/IP	27
	Conexiones de acceso remoto admitidas	28
	Plataformas compatibles	28
	Exploradores de web compatibles	29
	Aplicaciones admitidas de la consola de administración	29
	Compatibilidad con WS-Management	29
	Otros documentos que podrían ser útiles	31
2	Instalación y configuración del CMC	35
	Antes de comenzar	35
	Instalación del hardware del CMC	35
	Lista de verificación para la integración del chasis	36

Conexión básica del CMC a la red	37
Conexión en cadena tipo margarita del CMC a la red	37
Instalación del software de acceso remoto en una estación de administración	41
Instalación de RACADM en una estación de administración con Linux	41
Desinstalación de RACADM de una estación de administración con Linux	42
Configuración de un explorador de web	43
Servidor proxy	43
Filtro de suplantación de identidad de Microsoft	44
Obtención de la lista de revocación de certificados (CRL)	44
Descarga de archivos desde el CMC con Internet Explorer	45
Habilitación de animaciones en Internet Explorer	45
Configuración del acceso inicial al CMC	46
Configuración de la red del CMC	47
Configuración del sistema de red por medio del asistente de configuración del panel LCD	48
Acceso al CMC a través de una red	55
Instalación o actualización del firmware de la CMC	56
Descarga del firmware de la CMC	56
Actualización del firmware del CMC por medio de la interfaz web	57
Actualización del firmware del CMC mediante RADCAM	58
Configuración de las propiedades del CMC.	58
Configuración del presupuesto de alimentación.	58

Cómo establecer la configuración de red del CMC	59
Cómo agregar y configurar usuarios	59
Cómo agregar alertas de SNMP y por correo electrónico	59
Configuración de syslog remoto	60
Descripción del entorno de CMC redundante	60
Acerca del CMC en espera	61
Modo a prueba de fallas de CMC	61
Proceso de elección del CMC activo	63
Obtención del estado de la condición del CMC redundante	63
3 Configuración del CMC para el uso de consolas de línea de comandos	65
Funciones de la consola de línea de comandos en el CMC	65
Uso de una consola Serie, Telnet, o SSH	66
Uso de una consola Telnet con el CMC	66
Uso de SSH con el CMC	67
Activación de SSH en el CMC	67
Cambio del puerto de SSH	68
Activación del panel anterior para la conexión del iKVM	69
Configuración del software de emulación de terminal	69
Configuración de Minicom de Linux	69
Conexión a servidores o módulos de E/S con el comando connect	71

	Configuración del BIOS del servidor administrado para la redirección de la consola serie	73
	Configuración de Windows para la redirección de consola serie	73
	Configuración de Linux para la redirección de la consola serie del servidor durante el inicio	74
	Configuración de Linux para la redirección de la consola serie del servidor después del inicio	76
4	Uso de la interfaz de línea de comandos de RACADM	79
	Uso de una consola Serie, Telnet, o SSH	79
	Inicio de sesión en el CMC	80
	Inicio de una consola de texto	80
	Cómo utilizar de RACADM	80
	Subcomandos de RACADM.	81
	Acceso a RACADM de manera remota.	85
	Activación y desactivación de la capacidad remota de RACADM.	86
	Uso de RACADM de manera remota	86
	Mensajes de error de RACADM	87
	Uso de RACADM para configurar el CMC	87
	Configuración de las propiedades de red del CMC	88
	Configuración del acceso inicial al CMC.	88
	Cómo ver la configuración de red actual.	89
	Configuración de los valores de red de la LAN.	89
	Configuración de los valores de seguridad de la red (solo IPv4).	96
	Uso de RACADM para configurar usuarios	97
	Cómo agregar un usuario del CMC	98

Uso de RACADM para configurar la autenticación de claves públicas mediante SSH.	99
Generación de claves públicas para Windows	100
Generación de claves públicas para Linux.	101
Notas de la sintaxis de RACADM para CMC	101
Cómo ver las claves públicas	101
Cómo agregar claves públicas	102
Eliminación de claves públicas.	102
Inicio de sesión con autenticación de clave pública	102
Activación de un usuario del CMC con permisos	103
Desactivación de un usuario del CMC	103
Configuración de alertas de SNMP y por correo electrónico.	104
Configuración de múltiples CMC en varios chasis	104
Creación de un archivo de configuración del CMC.	105
Reglas de análisis	107
Modificación de la dirección IP del CMC	109
Uso de RACADM para configurar propiedades en el iDRAC	110
Solución de problemas	112
5 Uso de la interfaz web del CMC	115
Acceso a la interfaz web del CMC	115
Inicio de sesión.	116
Cierre de sesión	117
Configuración de los valores básicos del CMC.	117

Configuración de la ubicación física del chasis y el nombre del chasis	117
Establecimiento de la fecha y la hora en el CMC	118
Activación de soportes flash extraíbles	119
Página de condición del chasis	119
Cómo utilizar el grupo de chasis	120
Características del grupo de chasis	120
Cómo configurar un grupo de chasis.	121
Cómo eliminar un miembro del chasis principal.	122
Cómo desmontar un grupo de chasis.	123
Cómo desactivar un miembro del chasis miembro.	123
Cómo iniciar la página web del servidor o de un chasis miembro	124
Sincronización de un miembro nuevo con las propiedades del chasis principal	124
Inventario de blade para el grupo de MCM	125
Cómo guardar el informe de inventario de blade	125
Resumen de componentes del chasis	128
Gráficos del chasis	128
Condición del chasis	130
Información del componente seleccionado.	130
Supervisión del estado de la condición del sistema	137
Cómo ver los resúmenes del chasis y los componentes	137
Cómo ver el estado del presupuesto de alimentación	138

Cómo ver el nombre de modelo del servidor y etiqueta de servicio.	138
Cómo ver el estado de la condición de todos los servidores.	138
Edición de los nombres de ranuras	142
Uso del nombre de host del servidor como nombre de ranura.	143
Cómo establecer el primer dispositivo de inicio para los servidores.	143
Cómo ver el estado de la condición de un servidor individual	145
Cómo ver la condición de los módulos de E/S . . .	152
Cómo ver el estado de la condición de los ventiladores.	153
Cómo ver el estado del iKVM.	155
Cómo ver el estado de la condición de las unidades de suministro de energía	156
Cómo ver el estado de los sensores de temperatura.	158
Visualización del estado de la pantalla LCD	160
Cómo ver las identificaciones World Wide Name/Media Access Control (WWN/MAC).	161
Configuración de la red Fabric	161
Direcciones WWN/MAC	161
Configuración de las propiedades de red del CMC. . .	162
Configuración del acceso inicial al CMC.	162
Configuración de los valores de red de la LAN . .	162
Configuración de los valores de seguridad de la red del CMC	170
Configuración de VLAN	171
Cómo agregar y configurar usuarios del CMC	172
Tipos de usuarios.	173

Cómo agregar y administrar usuarios	180
Configuración y administración de los certificados de Microsoft Active Directory	182
Valores comunes	183
Configuración del esquema estándar	186
Configuración del esquema extendido	187
Administración de certificados de Active Directory	187
Archivo keytab de Kerberos	188
Configuración y administración de los servicios genéricos de protocolo ligero de acceso a directorios	189
Selección de servidores LDAP	191
Administración de la configuración de grupo de LDAP	192
Administración de certificados de seguridad de LDAP	192
Protección de las comunicaciones del CMC con certificados SSL y digitales	193
Capa de sockets seguros (SSL).	193
Solicitud de firma de certificado (CSR).	194
Acceso al menú principal de SSL.	195
Generación de una nueva solicitud de firma de certificado.	195
Carga de un certificado de servidor	199
Cargar clave y certificado de servidor de web.	200
Cómo ver un certificado de servidor	201
Administración de sesiones	201
Configuración de servicios	202

Configuración del presupuesto de alimentación	211
Administración de actualizaciones de firmware	212
Cómo ver las versiones actuales del firmware . . .	213
Actualización del firmware	214
Recuperación del firmware del iDRAC por medio del CMC	220
Actualización del firmware de los componentes de servidor mediante Lifecycle Controller	222
Administración del iDRAC	232
QuickDeploy de iDRAC	232
Configuración de la red de iDRAC	235
Inicio de la consola remota desde la interfaz gráfica de usuario de CMC	238
Cómo iniciar el iDRAC mediante el inicio de sesión único	239
Clonación de servidores	241
Captura de perfiles	241
Aplicación de perfiles	242
Visualización de la configuración del BIOS en el servidor	242
Gestión de perfiles almacenados	242
Registro de perfiles recientes	243
Estado de compleción y solución de problemas . .	243
FlexAddress	243
Cómo ver el estado de FlexAddress	244
Configuración de FlexAddress	248
Configuración FlexAddress para ranuras y redes Fabric a nivel del chasis	248
Configuración de FlexAddress de ranuras a nivel del servidor	249
Uso compartido de archivos remotos	250

	Preguntas frecuentes	253
	Solución de problemas del CMC	255
6	Uso de FlexAddress	257
	Activación de FlexAddress	258
	Verificación de la activación de FlexAddress	260
	Desactivación de FlexAddress	262
	Desactivación de FlexAddress	263
	Configuración de FlexAddress a través de la CLI	263
	Configuración adicional de FlexAddress para Linux	264
	Cómo ver el estado de FlexAddress a través de la CLI	265
	Configuración de FlexAddress a través de la interfaz gráfica de usuario	266
	Encendido en LAN con FlexAddress	266
	Solución de problemas de FlexAddress	266
	Mensajes de comandos	270
	CONTRATO DE LICENCIA DEL SOFTWARE DE DELL FlexAddress	273
	Preguntas frecuentes	277
7	Uso de FlexAddress Plus	279
	Activación de FlexAddress Plus	279
	Comparación de FlexAddress y FlexAddress Plus	280

8	Uso del servicio de directorio del CMC	281
	Uso del CMC con Microsoft Active Directory	281
	Extensiones de esquema de Active Directory	281
	Esquema estándar y esquema extendido	281
	Generalidades del esquema estándar de Active Directory	282
	Configuración de Active Directory con esquema estándar para acceder al CMC.	284
	Configuración del CMC con Active Directory de esquema convencional y la interfaz web	284
	Configuración del CMC con Active Directory de esquema convencional y RACADM	287
	Descripción general del esquema extendido.	288
	Extensiones de esquema de Active Directory	289
	Descripción general de las extensiones de esquema de RAC	289
	Descripción general de los objetos de Active Directory	290
	Configuración de Active Directory con esquema extendido para acceder al CMC.	294
	Cómo extender el esquema de Active Directory.	295
	Instalación de la extensión de Dell para el complemento Usuarios y equipos de Active Directory	301
	Cómo agregar usuarios y privilegios del CMC a Active Directory	302
	Configuración del CMC con Active Directory de esquema extendido y la interfaz web	305
	Configuración del CMC con Active Directory de esquema extendido y RACADM.	309

Preguntas frecuentes.	311
Configuración de inicio de sesión único	314
Requisitos del sistema	314
Configuración de valores	315
Configuración de Active Directory	316
Configuración del CMC	317
Cómo cargar el archivo keytab de Kerberos	317
Activación del inicio de sesión único.	317
Configuración del explorador para inicio de sesión único.	318
Conexión al CMC mediante inicio de sesión único	319
Configuración de la autenticación de dos factores de tarjeta inteligente.	320
Requisitos del sistema	321
Configuración de valores	321
Configuración de Active Directory	321
Configuración del CMC	321
Cómo cargar el archivo keytab de Kerberos	321
Activación de la autenticación de tarjeta inteligente	322
Configuración del explorador para el inicio de sesión mediante tarjeta inteligente	323
Cómo iniciar sesión en el CMC mediante una tarjeta inteligente	323
Solución de problemas del inicio de sesión mediante tarjeta inteligente	324
Uso del CMC con LDAP genérico	325
Configuración del directorio LDAP genérico para acceder a CMC	326
Configuración del servicio de directorio de LDAP genérico mediante la interfaz web del CMC	326

Selección de servidores LDAP	328
Administración de la configuración de grupo de LDAP	329
Administración de certificados de seguridad de LDAP	330
Configuración del servicio de directorio LDAP genérico mediante RACADM	330
Uso	331
Obtención de ayuda	331
9 Administración de la alimentación	333
Modo de redundancia de CA	334
Modo de redundancia de suministro de energía	336
Modo sin redundancia	337
Presupuesto de alimentación para módulos de hardware	338
Valores de prioridad de alimentación de ranura del servidor	341
Conexión dinámica del suministro de energía	342
Políticas de redundancia	344
Redundancia de CA	345
Redundancia de suministro de energía	345
Sin redundancia	345
Conservación de la energía y cambios en el presupuesto de alimentación	346
Cambios de suministro de energía y política de redundancia en el registro de sucesos del sistema	354
Estado de redundancia y condición general de la alimentación	356
Configuración y administración de la alimentación	356
Cómo ver el estado de la condición de las unidades de suministro de energía	356

Cómo ver el estado del consumo de alimentación	359
Cómo ver el estado del presupuesto de alimentación	364
Configuración del presupuesto y la redundancia de alimentación	369
Asignación de niveles de prioridad a los servidores	374
Cómo establecer el presupuesto de alimentación	375
Reducción de la alimentación del servidor para mantener el presupuesto de alimentación	376
Ejecución de operaciones de control de alimentación en el chasis	377
Ejecución de las operaciones de control de alimentación en un módulo de E/S	379
Ejecución de operaciones de control de alimentación en un servidor	380
Administración de la alimentación externa	382
Cómo utilizar de RACADM	384
Solución de problemas	385
10 Uso del módulo iKVM	387
Descripción general	387
Interfaz de usuario del iKVM	387
Security	387
Exploración	387
Identificación de servidores	388
Video	388
Plug and Play	388
Capacidad de actualización	388
Interfaces de conexión física	388

Prioridades de las conexiones del iKVM	389
Categorización por medio de la conexión de ACI	389
Uso de OSCAR	390
Conceptos básicos de navegación.	390
Configuración de OSCAR	391
Administración de servidores con iKVM	394
Compatibilidad con periféricos.	394
Cómo ver y seleccionar servidores	395
Configuración de la seguridad de la consola	398
Exploración del sistema	403
Transmisión a servidores.	405
Administración del iKVM desde el CMC	406
Activación o desactivación del panel anterior.	406
Activación de la consola de CMC de Dell a través de iKVM	407
Cómo ver el estado y las propiedades del iKVM	407
Actualización del firmware de iKVM.	409
Solución de problemas	411
11 Administración de la red Fabric de E/S	415
Administración de la red Fabric.	416
Configuraciones no válidas	417
Configuración no válida de tarjeta mezzanine	418
Configuración no válida de módulo de E/S y tarjeta mezzanine.	418
Configuración no válida de módulo de E/S y módulo de E/S	418

Situación de encendido por primera vez	419
Supervisión de la condición del módulo de E/S.	419
Cómo ver el estado de la condición de un módulo de E/S individual	423
Configuración de valores de red para un módulo de E/S individual	425
Solución de problemas de los valores de red del módulo de E/S.	427
12 Solución de problemas y recuperación	429
Descripción general	429
Herramientas de supervisión del chasis	430
Recopilación de información de configuración, registros y estado del chasis	430
Uso	430
Interfaces admitidas	430
RACDUMP mediante CLI	431
RACDUMP remoto	431
Uso de RACDUMP remoto	432
RACDUMP mediante Telnet.	432
Configuración de los LED para identificar componentes en el chasis	433
Cómo configurar alertas SNMP	434
Descarga del archivo MIB (Base de información de administración) SNMP	440
Configuración de alertas por correo electrónico	441
Primeros pasos para solucionar problemas en un sistema remoto	444

Supervisión de la alimentación y ejecución de los comandos de control de alimentación en el chasis . . .	445
Cómo ver el estado del presupuesto de alimentación	445
Ejecución de una operación de control de alimentación	445
Solución de problemas de energía	446
Administración de trabajos de Lifecycle Controller en un sistema remoto.	449
Cómo ver los resúmenes del chasis.	450
Cómo ver el estado de la condición del chasis y de los componentes.	454
Cómo ver los registros de sucesos	455
Cómo ver el registro de hardware	455
Cómo ver el registro del CMC	458
Uso de la consola de diagnósticos	459
Restablecimiento de componentes	460
Solución de problemas de errores de protocolo de hora de red (NTP)	463
Interpretación de los colores y los patrones de parpadeo de los LED.	465
Solución de problemas de un CMC que no responde.	469
Observación de los LED para aislar el problema	469
Obtención de la información de recuperación desde el puerto serie DB-9.	470
Recuperación de la imagen del firmware	471
Solución de problemas de red.	472

Restablecimiento de la contraseña de administrador olvidada	472
Cómo guardar y restablecer los valores de configuración y certificados del chasis.	476
Solución de problemas de alertas.	476
13 Diagnósticos	477
Uso de la interfaz del panel LCD.	477
Navegación de la pantalla LCD	477
Menú principal	478
Menú de configuración del LCD	479
Pantalla de configuración de idioma	479
Pantalla predeterminada	479
Pantalla de estado gráfico del servidor	480
Pantalla de estado gráfico del módulo	481
Pantalla del menú Gabinete	481
Pantalla de estado del módulo	482
Pantalla Estado del gabinete	482
Pantalla de resumen de IP	482
Diagnósticos	483
Solución de problemas del hardware LCD	483
Mensajes de la pantalla LCD del panel anterior	486
Mensajes de error de la pantalla LCD.	486
Información de estado del servidor y módulo de LCD	493
Índice	499

Descripción general

Dell Chassis Management Controller (CMC) es una solución de hardware y software de acoplamiento activo para la administración de sistemas diseñada para proporcionar las siguientes funciones en los sistemas de chasis Dell PowerEdge M1000e:

- Capacidades de administración remota
- Control de alimentación
- Control de enfriamiento

El CMC, que tiene su propio microprocesador y memoria, recibe alimentación del chasis modular en el que está conectado. Para comenzar con el CMC, ver “Instalación y configuración del CMC” en la página 35.

El CMC proporciona funciones de administración de varios sistemas para servidores blade. Las principales funciones del CMC son la administración térmica y de alimentación.

- Administración térmica y de energía automática en tiempo real de nivel de alojamiento.
 - El CMC controla los requisitos de alimentación del sistema y admite el modo opcional Conexión dinámica del suministro de energía. Esto permite al CMC activar los suministros de energía o ponerlos en espera de forma dinámica, según los requisitos de carga y redundancia, para mejorar la eficiencia energética.
 - El CMC informa del 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 módulos de alta densidad 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:
 - Los ajustes de red y de seguridad del alojamiento M1000e.
 - Los ajustes de redundancia de alimentación y de límite de energía.
 - Los ajustes de red de iDRAC y de los conmutadores de E/S.
 - El primer dispositivo de inicio de los módulos de alta densidad del servidor.
 - Comprueba la coherencia de la red Fabric de E/S entre los módulos de E/S y los servidores blade, y deshabilita componentes (si procede) para proteger el hardware del sistema.
 - La seguridad de acceso de los usuarios.

El CMC se puede configurar para que envíe alertas por correo electrónico o alertas de capturas SNMP para advertencias o errores relacionados con temperaturas, configuraciones erróneas de hardware, interrupciones de la alimentación y velocidades de los ventiladores.

El chasis M1000e se puede configurar con un solo CMC o con CMC redundantes. En las configuraciones de CMC redundantes, si el primer CMC pierde la comunicación con el chasis M1000e o la red de administración, el CMC en espera se hace cargo de la administración del chasis.

Novedades de esta versión

Esta versión del CMC admite las funciones siguientes:

- Almacenamiento y restauración de la configuración del chasis.
- Registro SEL mejorado.
- Tarjeta de red secundaria Broadcom 57810-k de dos puertos y 10 GB.
- Tarjeta mezzanine Broadcom 57810-k de dos puertos y 10 GB.
- Tarjeta mezzanine Intel I350 de cuatro puertos y 1 Gb.
- Tarjeta de red secundaria Intel x520-k de dos puertos y 10 GB.
- Tarjeta mezzanine Intel x520-k de dos puertos y 10 GB.
- Tarjeta de red secundaria Qlogic QMD8262-k de dos puertos y 10 Gb.
- Conmutador de Infiniband QDR/DDR Mellanox M4001Q.
- Conmutador de InfiniBand FDR Mellanox M4001F.
- Tarjeta mezzanine de InfiniBand QDR/DDR Mellanox ConnectX-3.

- Tarjeta mezzanine de InfiniBand FDR Mellanox ConnectX-3.
- MIB de CMC expandida para incluir OID para la ubicación física del chasis.
- MIB de CMC expandida para incluir OID para la etiqueta de servicio y el nombre de ranura del servidor blade.
- Admite la administración de la alimentación externa a través de **Open Manage Power Connect** (OMPC).
- Replicación de uno a varios ajustes de servidor BIOS para servidores iDRAC6 e iDRAC7 (clonación de servidores).
- Capacidad añadida a la función Administración de múltiples chasis para la sincronización de las propiedades del nuevo miembro con las del chasis principal.
- Compatible con el servidor iDRAC7 PowerEdge M620 inicial.
- Información de la CPU y la memoria disponible en la interfaz gráfica de usuario para servidores compatibles con **Lifecycle Controller** (LC).
- Admite la creación de inventarios de servidores y módulos de E/S, así como la generación de informes para un grupo de MCM (administración de múltiples chasis).

Funciones de administración del CMC

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 del 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 del 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 por medio de 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. Para obtener más información, ver “Uso de FlexAddress” en la página 257.
- Gráfico de la condición y del estado de componentes del chasis.
- Asistencia para servidores simples o de varias ranuras.
- El asistente de configuración iDRAC con LCD admite la configuración de la red del iDRAC.
- Inicio de sesión único de iDRAC.
- Compatibilidad para el protocolo de hora de red (NTP).
- Resumen del servidor, informe de la alimentación y páginas de control de alimentación mejorados.
- Protección forzada contra fallas del CMC y recolocación virtual de servidores.
- Administración de múltiples chasis, que permite que desde el chasis principal sean visibles hasta 8 otros chasis.

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.
- Autenticación del usuario mediante Active Directory (opcional) o identificaciones y contraseñas de usuario almacenadas en el hardware.
- Autoridad basada en funciones, que permite que el administrador configure privilegios específicos para cada usuario.
- Configuración de identificaciones y contraseñas de usuario por medio de la interfaz web.
- La interfaz web admite cifrado SSL 3.0 de 128 bits y cifrado SSL 3.0 de 40 bits (para países en los que no se admiten 128 bits).



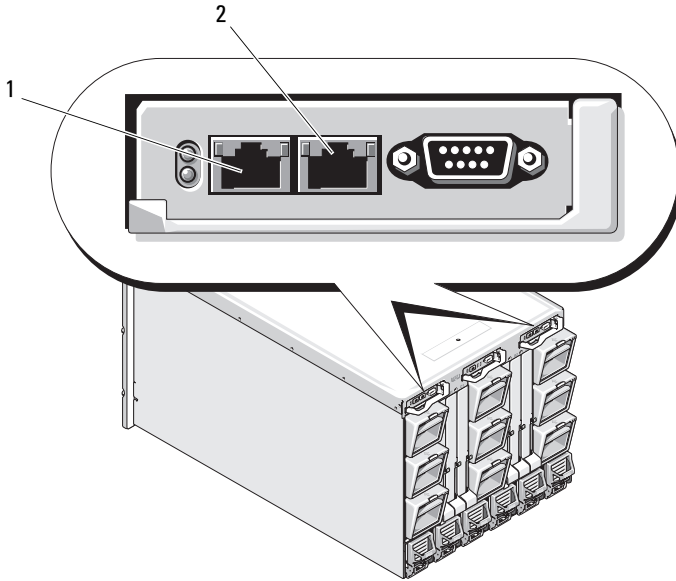
NOTA: Telnet no admite el cifrado SSL.

- Puertos IP configurables (si procede).
- 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, autenticación de dos factores y autenticación de clave pública.

Descripción general del chasis

La Ilustración 1-1 muestra el borde delantero de un CMC (inserto) y las ubicaciones de las ranuras del CMC en el chasis.

Ilustración 1-1. Chasis y CMC Dell M1000e



1 Puerto GB

2 Puerto STK

Especificaciones del hardware

En la siguiente sección se proporciona información sobre las especificaciones de hardware del CMC.

Puertos TCP/IP

Debe proporcionar la información del puerto al abrir servidores de seguridad para tener acceso remoto a un CMC.

Tabla 1-1. Puertos de detección de servidores del CMC

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

* Puerto configurable

Tabla 1-2. 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

Conexiones de acceso remoto admitidas

En la Tabla 1-3 se listan las controladoras Remote Access Controller admitidas.

Tabla 1-3. Conexiones de acceso remoto admitidas

Conexión	Características
Puertos de la interfaz de red de CMC	<ul style="list-style-type: none">• 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 consolidación de cables entre chasis• STK: puerto de vínculo superior para la consolidación de cables entre chasis de la red de administración• Ethernet de 10 Mbps/100 Mbps/1 Gbps a través del puerto GbE del CMC• Compatibilidad con DHCP• Notificación de sucesos por correo electrónico y capturas SNMP• Interfaz de red para el iDRAC y los módulos de E/S• Compatibilidad con la consola de comandos Telnet/SSH y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado
Puerto serie	<ul style="list-style-type: none">• Compatibilidad con la consola serie y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado• 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 módulo de E/S, mediante el comando <code>connect</code> (o <code>racadm connect</code>)
Otras conexiones	<ul style="list-style-type: none">• Acceso a la consola del CMC de Dell por medio del módulo de conmutador KVM integrado Avocent (iKVM)

Plataformas compatibles

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

Para ver las últimas plataformas admitidas, consulte la *Dell Systems Software Support Matrix* que se encuentra en support.dell.com/manuals.

Exploradores de web compatibles

Los siguientes exploradores web son compatibles con CMC 4.0:

- Microsoft Internet Explorer 8.0 para Windows 7, Windows Vista, Windows XP y la familia de Windows Server 2003.
- Microsoft Internet Explorer 7.0 para Windows 7, Windows Vista, Windows XP y la familia de Windows Server 2003.
- Mozilla Firefox 1.5 (32 bits): funcionalidad limitada.

Para obtener información actualizada sobre los exploradores web compatibles con CMC 4.0, consulte la *Dell Systems Software Support Matrix* disponible en el sitio support.dell.com/manuals.

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 deseada en el menú desplegable **Su idioma (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 la página web de asistencia de Dell en support.dell.com/manuals.

Compatibilidad con WS-Management

Servicios web para administración (WS-MAN) es un protocolo basado en el protocolo simple de acceso a objetos (SOAP) que se utiliza en la administración de sistemas. WS-MAN proporciona un protocolo de interoperabilidad para que los dispositivos puedan compartir e intercambiar datos entre distintas redes. CMC utiliza WS-MAN para transmitir información de administración basada en el Modelo común de información (CIM) del Grupo de trabajo de administración distribuida (DMTF). La información de CIM define la semántica y los tipos de información que pueden manipularse en un sistema administrado. Las interfaces de administración de la plataforma del servidor incorporado Dell se organizan en perfiles, donde cada perfil define las interfaces específicas para un dominio de administración o área de funcionalidad determinados. Además, Dell ha definido diversas extensiones de modelo y perfil que ofrecen interfaces para otras capacidades.

El acceso a WS-Management exige iniciar sesión mediante privilegios de usuario local con autenticación básica por el protocolo de capa de conexión segura (SSL) en el puerto 443. Para obtener información sobre cómo configurar cuentas de usuario, consulte la sección de propiedad de base de datos Session Management en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Los datos disponibles mediante WS-Management son un subconjunto de datos proporcionados por la interfaz de instrumentación del CMC asignada a los siguientes perfiles de DMTF versión 1.0.0:

- Perfil de capacidades de asignación
- Perfil métrico básico
- Perfil básico del servidor
- Perfil de sistema computacional
- Perfil de sistema modular
- Perfil de propiedad física
- Perfil de asignación de alimentación de Dell
- Perfil de suministro de energía de Dell
- Perfil de topología de la alimentación de Dell
- Perfil de administración del estado de la alimentación
- Perfil de registro de perfiles
- Perfil de registro
- Perfil de asignación de recursos
- Perfil de autorización basada en funciones
- Perfil de sensores
- Perfil de procesador de servicio
- Perfil de administración de identidad simple
- Perfil del cliente de Active Directory de Dell
- Perfil de control de inicio
- Perfil de NIC simple de Dell

La implementación de WS-MAN del CMC utiliza SSL en el puerto 443 para seguridad del transporte y admite la autenticación básica. Para obtener información sobre cómo configurar cuentas de usuario, consulte la sección de propiedad de base de datos *Session Management en la RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC). 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 la conexión cliente por medio de Microsoft WinRM, se requiere la versión 2.0 como mínimo. Para obtener más información, consulte el artículo de Microsoft <<http://support.microsoft.com/kb/968929>>.

Se ofrecen guías de implementación adicionales, documentos técnicos, muestras de perfiles y códigos, disponibles en Dell Tech Center: www.delltechcenter.com. Para obtener más información, ver:

- Sitio web de DMTF: www.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

Otros documentos que podrían ser útiles

Además de esta guía, puede consultar las siguientes guías disponibles en support.dell.com/manuals. En la página Manuales, haga clic en **Software**→**Systems Management**. Haga clic en el vínculo del producto correspondiente que se encuentra a la derecha para tener acceso a los documentos:

- *La ayuda en línea para el CMC* proporciona información sobre el uso de la interfaz web.
- Las *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* (Especificaciones técnicas de la tarjeta Secure Digital (SD) de Chassis Management Controller [CMC]) proporcionan información mínima sobre el uso, la instalación y la versión del BIOS y el firmware.

- La *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide* (Guía del usuario de Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise para servidores blade) ofrece información sobre la instalación, la configuración y el mantenimiento del iDRAC en sistemas administrados.
- La *Guía del usuario de Dell OpenManage IT Assistant* ofrece información sobre IT Assistant.
- Documentación específica para la aplicación de consola de administración de otros fabricantes.
- La *Guía del usuario de Dell OpenManage Server Administrator* contiene información sobre cómo instalar y utilizar Server Administrator.
- La *Guía del usuario de Dell Update Packages* proporciona información acerca de cómo obtener y utilizar Dell Update Packages como parte de su estrategia de actualización del sistema.

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

- En las instrucciones de seguridad incluidas con el sistema se proporciona información importante sobre normativas y seguridad. Para obtener más información sobre normativas, visite la página de inicio sobre cumplimiento de normativas en www.dell.com/regulatory_compliance. La información sobre la garantía puede estar incluida en este documento o constar en un documento aparte.
- En los documentos *Rack Installation Guide* (Guía de instalación en bastidor) e *Rack Installation Instructions* (Instrucciones de instalación en bastidor) que se incluyen con el bastidor se describe cómo instalar el sistema en un bastidor.
- En el *Manual del propietario de hardware*, se proporciona información acerca de las funciones del sistema y se describe cómo solucionar problemas del sistema e instalar o sustituir componentes.
- En la documentación del software de administración de sistemas se describen las 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 la versión o archivos léame para proporcionar actualizaciones de última hora relativas al sistema o a la documentación, o material avanzado de consulta técnica destinado a técnicos o usuarios experimentados.
- Para obtener más información sobre la configuración de red del módulo de E/S, consulte el documento *Información importante del conmutador Dell PowerConnect M6220* y el *Documento técnico del agregador de puertos Dell PowerConnect de la serie 6220*.

Algunas veces, con el sistema se incluyen actualizaciones que describen los cambios realizados en el sistema, en el software o en la documentación. Lea siempre las actualizaciones primero, puesto que a menudo sustituyen la información contenida en otros documentos.

Instalación y configuración del CMC

Esta sección proporciona información acerca de cómo instalar el hardware del CMC, cómo establecer el acceso al CMC, cómo configurar el entorno de administración para utilizar el CMC, y guía a través de los siguientes pasos para configurar el CMC:

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

Para obtener más información sobre la instalación y la configuración de entornos de CMC redundantes, ver “Descripción del entorno de CMC redundante” en la página 60.

Antes de comenzar

Antes de configurar el entorno del CMC, descargue la versión más reciente del firmware del CMC del sitio web del servicio de asistencia Dell Support en support.dell.com.

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

Instalación del hardware del CMC

El CMC está preinstalado en el chasis, por lo que no se requiere instalación. Puede instalar un segundo CMC para que funcione como dispositivo en espera para el CMC activo. Para obtener más información sobre un CMC en espera, ver “Descripción del entorno de CMC redundante” en la página 60.

Lista de verificación para la integración del chasis

Los siguientes pasos permiten configurar el chasis con precisión:

- 1 El CMC y la estación de administración en la que se utilice el explorador deben estar en la misma red, que se denomina la red de administración. Conecte un cable de red Ethernet del puerto CMC que tenga la etiqueta **GB** a la red de administración.



NOTA: No coloque un cable en el puerto Ethernet del CMC que tiene la etiqueta **STK**. Para obtener más información sobre la conexión del puerto **STK**, ver “Descripción del entorno de CMC redundante” en la página 60.

- 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 disponible en la esquina inferior izquierda del chasis o encienda el chasis desde la interfaz gráfica de usuario del CMC después de completar el paso 7.



NOTA: No encienda los servidores.

- 6 Por medio del panel LCD que se encuentra en la parte anterior del sistema, dé una dirección IP estática al CMC o configúrelo para DHCP.
- 7 Conéctese a la dirección IP del CMC a través del explorador web con el nombre de usuario (**root**) y la contraseña (**calvin**) predeterminados.
- 8 Proporcione una dirección IP a cada iDRAC en la interfaz gráfica de usuario 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 gráfica de usuario del CMC.
- 10 Establezca conexión con cada iDRAC a través del explorador web y realice la configuración final del iDRAC. El nombre de usuario predeterminado es **root** y la contraseña predeterminada es **calvin**.
- 11 Establezca conexión con cada módulo de E/S a través del explorador web y realice la configuración final del módulo de E/S.
- 12 Encienda los servidores e instale el sistema operativo.

Conexión básica del CMC a la red

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

Cada CMC tiene dos puertos RJ-45 Ethernet, designados **GB** (el puerto de *vínculo superior*) y **STK** (el puerto de *apilamiento* o de consolidación de cables). Con una conexión de cables básica, se conecta el puerto GB a la red de administración y se deja el puerto STK sin utilizar.

△ PRECAUCIÓN: Conectar el puerto STK a la red de administración puede producir resultados impredecibles. La conexión de los puertos GB y STK a la misma red (dominio de difusión) puede causar una tormenta de difusión.

Conexión en cadena tipo margarita del CMC a la red

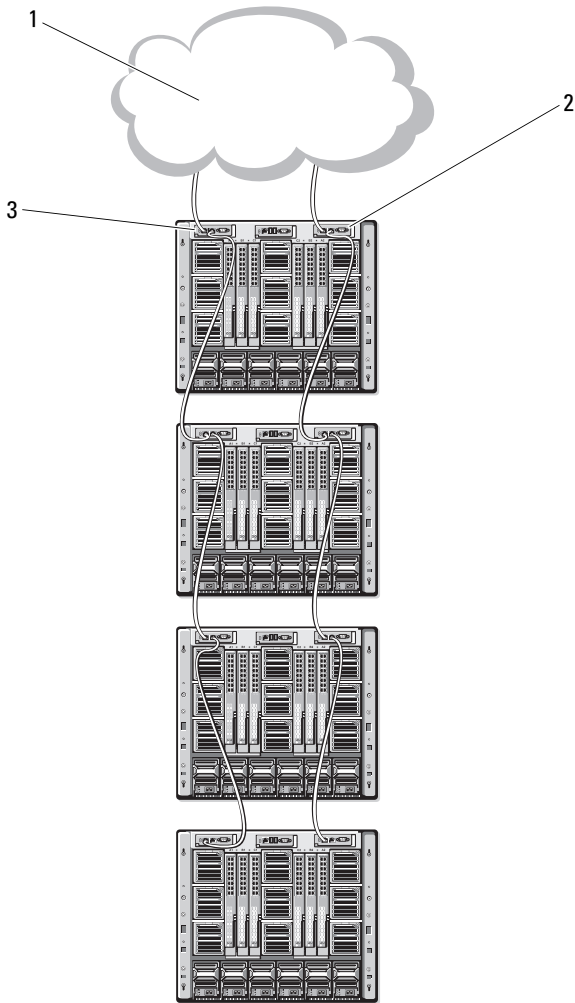
Si tiene varios chasis en un estante, puede reducir el número de conexiones a la red de administración conectando hasta cuatro chasis entre sí en una cadena margarita. Si cada uno de los cuatro chasis tiene un CMC redundante, al conectarlos en una cadena tipo margarita el número de conexiones requeridas de la red de administración se reduce de ocho a dos. Si cada chasis tiene solo un CMC, las conexiones requeridas pueden reducirse de cuatro a una.

Cuando se conectan varios chasis entre sí en cadena tipo margarita, GB es el puerto de vínculo superior y STK es el puerto de apilamiento (consolidación de cables). Conecte los puertos GB a la red de administración o al puerto STK del CMC en el chasis que esté más cerca de la red. El puerto STK solo debe conectarse a un puerto GB posterior a la cadena o la red.

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

La Ilustración 2-1 muestra la disposición de los cables para cuatros chasis conectados en cadena tipo margarita, cada uno con CMC activos y en espera.

Ilustración 2-1. Conexión en cadena tipo margarita del CMC a la red



- 1 Red de administración
- 2 CMC en espera
- 3 CMC activo

La Ilustración 2-2, la Ilustración 2-3 y la Ilustración 2-4 muestran ejemplos de conexiones incorrectas del CMC.

Ilustración 2-2. Cableado incorrecto para la conexión de red de CMC: dos CMC

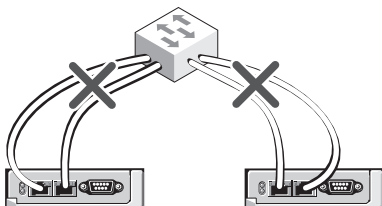


Ilustración 2-3. Cableado incorrecto para la conexión de red de CMC: un CMC

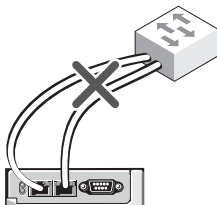
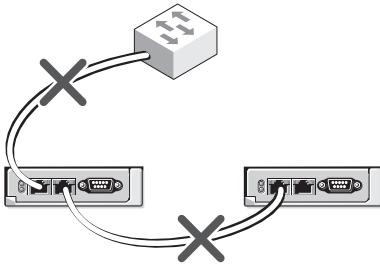


Ilustración 2-4. Cableado incorrecto para la conexión de red de CMC: dos CMC



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 tiene un tercer chasis, conecte el puerto GB del CMC activo al puerto STK del CMC activo en el segundo chasis.
- 4 Si tiene un cuarto chasis, conecte el puerto GB del CMC activo al puerto STK del tercer chasis.
- 5 Si tiene CMC redundantes en el chasis, conéctelos siguiendo 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 en otro chasis. Conectar un puerto STK a la red de administración puede interrumpir la red y provocar 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: Nunca conecte un CMC 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.

Para comenzar con el CMC, ver “Instalación del software de acceso remoto en una estación de administración” en la página 41.

Instalación del software de acceso remoto en una estación de administración

Puede acceder al CMC desde una estación de administración por medio de 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 System Build and Update Utility.
- SYSMGMT: contiene productos de software de administración de sistemas, incluso Dell OpenManage Server Administrator.
- Docs: contiene documentación para sistemas, productos de software de administración de sistemas, periféricos y controladoras RAID.
- SERVICE: contiene las herramientas requeridas 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 la *Dell OpenManage Installation and Security User's Guide* (Guía del usuario de instalación y seguridad de Dell OpenManage) disponible en el DVD o en support.dell.com/manuals. También puede descargar la última versión de las herramientas del DRAC Tools de support.dell.com.

Instalación de RACADM en una estación de administración con Linux

- 1 Inicie sesión como root 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 iniciar ningún archivo ejecutable desde el DVD. Deberá montar manualmente el DVD-ROM y después ejecutar los archivos ejecutables.

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

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

- 5 Para recibir ayuda en relación con el comando `RACADM`, escriba `racadm help` después de ejecutar los comandos anteriores. Para obtener más información sobre `RACADM`, ver “Uso de la interfaz de línea de comandos de `RACADM`” en la página 79.



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

```
racadm getconfig -f <nombre de archivo>
```

Para obtener más información sobre `RACADM` remoto, ver “Acceso a `RACADM` de manera remota” en la página 85 y las secciones subsiguientes.

Desinstalación de `RACADM` de una estación de administración con Linux

- 1 Inicie sesión como `root` en el sistema en el que desea instalar los componentes de Management Station.
- 2 Utilice 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 de web

Puede configurar y administrar el CMC y los servidores y módulos instalados en el chasis por medio de un explorador de web. Consulte la sección *Exploradores admitidos* en la *Dell Systems Software Support Matrix* que se encuentra en: support.dell.com/manuals.

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



NOTA: Asegúrese de que las medidas de seguridad en la red de administración, como los servidores de seguridad y los servidores proxy, no impidan al explorador web acceder al CMC.

Las funciones de algunos exploradores pueden interferir con la conectividad o el rendimiento, en especial si la red de administración no tiene una ruta a Internet. Si la estación de administración está ejecutando un sistema operativo Windows, hay configuraciones de Internet Explorer que pueden interferir con la conectividad, incluso cuando se utiliza una interfaz de línea de comandos para acceder a la red de administración.

Servidor proxy

Para navegar a través de un servidor proxy que no tiene acceso a la red de administración, puede agregar las direcciones de la red de administración a la lista de excepciones del explorador. Esto indica al explorador que omita el servidor proxy cuando accede a la red de administración.

Internet Explorer

Para editar la lista de excepciones en Internet Explorer:

- 1 Inicie Internet Explorer.
- 2 Haga clic en **Herramientas**→ **Opciones de Internet**→ **Conexiones**.
- 3 En la sección **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.
- 4 En la sección **Servidor proxy**, haga clic en **Opciones avanzadas**.
- 5 En la sección **Excepciones**, agregue a la lista las direcciones de los CMC y los iDRAC en la red de administración, separadas por punto y coma. Puede utilizar nombres DNS y comodines en sus 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 Windows) o bien haga clic en **Edición**→ **Preferencias** (para Linux).
- 3 Haga clic en **Avanzadas** y luego en la ficha **Red**.
- 4 Haga clic en **Configuración**.
- 5 Seleccione la opción **Configuración manual del proxy**.
- 6 En el campo **No usar proxy para**, escriba las direcciones de los CMC y los iDRAC en la red de administración, separadas por comas. Puede utilizar nombres DNS y comodines en sus anotaciones.

Filtro de suplantación de identidad de Microsoft

Si el Filtro de suplantación de identidad (phishing) de Microsoft está activado 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 utiliza el explorador u otra interfaz como RACADM remoto. Siga estos pasos para desactivar el filtro de suplantación de identidad:

- 1 Inicie Internet Explorer.
- 2 Haga clic en **Herramientas**→ **Filtro de suplantación de identidad** y luego haga clic en **Configuración del filtro de suplantación de identidad**.
- 3 Marque la casilla **Desactivar el filtro de suplantación de identidad** y haga clic en **Aceptar**.

Obtención de la lista de revocación de certificados (CRL)

Si el CMC no tiene una ruta a Internet, usted debe desactivar la función de obtención de la lista de revocación de certificados (CRL) en Internet Explorer. Esta función comprueba si un servidor como el Web Server del CMC utiliza un certificado que está en una lista de certificados revocados obtenida de Internet. Si no hay acceso a Internet, esta función puede provocar demoras de varios segundos al momento de acceder al CMC por medio del explorador o con una interfaz de línea de comandos, como RACADM remoto.

Para desactivar la obtención de la CRL:

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

Descarga de archivos desde el CMC con Internet Explorer

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

Siga estos pasos para activar la opción **No guardar las páginas cifradas en el disco**:

- 1 Inicie Internet Explorer.
- 2 Haga clic en **Herramientas**→ **Opciones de Internet**, luego haga clic en **Opciones avanzadas**.
- 3 Desplácese a la sección Seguridad y seleccione **No guardar las páginas cifradas en el disco**.

Habilitación de animaciones en Internet Explorer

Al transferir archivos a una interfaz web o desde esta, un icono de transferencia de archivos gira para mostrar que hay actividad de transferencia. En Internet Explorer, esto requiere que el explorador esté configurado para reproducir animaciones, que es la configuración predeterminada.

Para configurar Internet Explorer para reproducir animaciones:

- 1 Inicie Internet Explorer.
- 2 Haga clic en **Herramientas**→ **Opciones de Internet**, luego haga clic en **Opciones avanzadas**.
- 3 Desplácese a la sección Multimedia y marque **Activar animaciones en páginas web**.

Configuración del acceso inicial al CMC

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



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

Para obtener información sobre la configuración de los valores de la red del CMC, ver “Configuración de la red del CMC” en la página 47. Esta configuración inicial asigna los parámetros del sistema de red TCP/IP para permitir el acceso al CMC.

El CMC y el iDRAC en cada servidor y los puertos de administración de red de todos los módulos de E/S de conmutador están conectados 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 está conectado 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.



NOTA: Se recomienda aislar la administración del chasis de la red de datos. Dell no puede proporcionar asistencia ni garantías respecto del tiempo de funcionamiento de un chasis que no está correctamente integrado al entorno. Debido al potencial del tráfico de la red de datos, las interfaces de administración en la red de administración interna pueden saturarse por el tráfico dirigido a los servidores. Esto ocasiona demoras en las comunicaciones de CMC e iDRAC. Las demoras pueden causar un comportamiento impredecible del chasis, por ejemplo, que el CMC muestre al iDRAC fuera de línea aun cuando está encendido y en funcionamiento, lo que a su vez genera otros comportamientos no deseados. Si no es práctico aislar físicamente la red de administración, la otra opción es enviar el tráfico de CMC y de iDRAC a una VLAN separada. Las interfaces de red del iDRAC individuales y del CMC puede configurarse para usar una VLAN con el comando `racadm setniccfg`. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos de iDRAC6 y CMC).

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

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

Para obtener más información sobre la conexión en cadena margarita, ver “Conexión en cadena tipo margarita del CMC a la red” en la página 37.



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.

Configuración de la red del CMC



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

Puede realizar la configuración inicial de red del CMC antes o después de que el CMC tenga una dirección IP. Si establece la configuración inicial de red del CMC *antes* de tener una dirección IP, puede utilizar cualquiera de las siguientes interfaces:

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

Si define la configuración inicial de red *después* de que el CMC tenga una dirección IP, puede utilizar cualquiera de las siguientes interfaces:

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

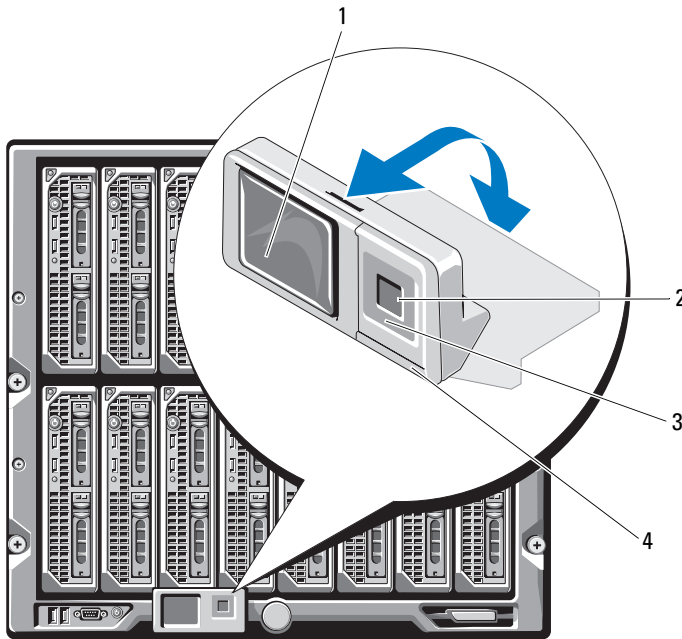
Configuración del sistema de red por medio del asistente de configuración del panel LCD

NOTA: La opción de configurar el CMC mediante el asistente de configuración de LCD solo estará disponible hasta que se instale el CMC o se cambie la contraseña predeterminada. Si no se cambia la contraseña, se puede continuar usando el LCD para reconfigurar el CMC, lo cual provocaría un posible riesgo de seguridad.

El panel LCD se encuentra en la esquina inferior izquierda en el frente del chasis.

La Ilustración 2-5 muestra el panel LCD.

Ilustración 2-5. Pantalla LCD



- | | | | |
|---|-------------------------------|---|-------------------------|
| 1 | Pantalla LCD | 2 | Botón de selección |
| 3 | Botones de desplazamiento (4) | 4 | LED indicador de estado |

La pantalla LCD muestra menús, iconos, imágenes y mensajes.

El LED indicador de estado en el panel LCD indica la condición general del chasis y de los componentes de este.

- 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.

Navegación en la pantalla LCD

El lado derecho del panel LCD tiene cinco botones: cuatro botones de flecha (hacia arriba, abajo, izquierda y derecha) y un botón central.

- *Para moverse de una pantalla a otra*, utilice los botones de flecha hacia la derecha (siguiente) y hacia la izquierda (anterior). Puede regresar a la pantalla anterior en cualquier momento mientras utiliza el asistente de configuración.
- *Para desplazarse a través de las opciones en una pantalla*, utilice los botones de flecha hacia abajo y hacia arriba.
- *Para seleccionar y guardar un elemento en una pantalla y avanzar a la siguiente pantalla*, utilice el botón central.

Para obtener más información sobre cómo utilizar el panel LCD, consulte la sección del panel LCD en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Uso del asistente de configuración de LCD

Para configurar una red con el asistente de configuración de LCD:

- 1** Si aún no lo ha hecho, presione el botón de encendido del chasis para encenderlo.

La pantalla LCD muestra una serie de pantallas de inicialización conforme se enciende. Cuando está listo, muestra la pantalla

Configuración de idioma.

- 2** Seleccione su idioma con los botones de flecha y luego presione el botón central para seleccionar **Aceptar/Sí** y presione nuevamente el botón central.

- 3 Aparecerá la pantalla **Gabinete** con la siguiente pregunta: **¿Desea configurar el gabinete?**
 - a Presione el botón central para avanzar a la pantalla **Configuración de red del CMC**. Ver paso 4.
 - b Para salir del menú **Configuración del gabinete**, seleccione el icono **NO** y presione el botón central. Ver paso 9.
- 4 Presione el botón central para avanzar a la pantalla **Configuración de red del CMC**.
- 5 Seleccione la velocidad de la red (10 Mbps, 100 Mbps, Automática [1 Gbps]) con el botón de flecha hacia abajo.



NOTA: Para que el rendimiento de la red sea efectivo, el valor de Velocidad de la red deberá 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 aumentará y la comunicación por medio de la red se hará 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**.

- 6 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 Activado o si se selecciona 1000 MB (1 Gbps).



NOTA: 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. Esta incompatibilidad de la configuración de dúplex provocará que la conexión de red sea lenta.

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

- 7 Seleccione el protocolo de Internet (IPv4, IPv6 o ambos) que desea usar para el CMC.

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

- 8** Seleccione el modo en el que desea que el CMC obtenga las direcciones IP del NIC:

Dynamic Host Configuration Protocol
(Protocolo de configuración dinámica de host)

El CMC obtiene la configuración IP (dirección IP, máscara y puerta de enlace) automáticamente desde un servidor DHCP en la red. El CMC tendrá asignada una dirección IP exclusiva en toda la red. Si ha seleccionado la opción DHCP, presione el botón central. Aparecerá la pantalla **¿Desea configurar el iDRAC?** Vaya al paso 10.

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** y después:

- a** Establezca la **Dirección IP estática** con las teclas de flecha hacia la derecha o 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 estática**, presione el botón central para continuar.
- b** Establezca la máscara de subred y luego presione el botón central.
- c** Establezca la puerta de enlace y luego presione el botón central. Aparece la pantalla **Resumen de la red**.

La pantalla **Resumen de la red** muestra los valores de la **Dirección IP estática**, la **Máscara de subred** y la **Puerta de enlace** que usted introdujo. Compruebe que los valores sean correctos. Para corregir un valor, vaya al botón de flecha hacia la izquierda y luego presione la tecla central para regresar a la pantalla de ese valor. Después de hacer una corrección, presione el botón central.

- d** Cuando haya confirmado que los valores introducidos son correctos, presione el botón central. Aparecerá la pantalla **¿Desea registrar el DNS?** Aparece la pantalla.



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

- 9** 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 **¿Desea registrar el DNS?** Vaya al paso 10.

Establezca la **Dirección IP de DNS** con las teclas de flecha hacia la derecha o 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.

- 10** 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.

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

Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de host)

El iDRAC recupera la configuración IP (dirección IP, máscara y puerta de enlace) automáticamente desde un servidor DHCP en la red. Se asignará al iDRAC una dirección IP exclusiva en toda la red. Presione el botón central.

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** y después:

- a** Establezca la **Dirección IP estática** con las teclas de flecha hacia la derecha o 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 de IP estática de cada iDRAC posterior se calculará como un incremento de número de la ranura de esta dirección IP. Cuando haya terminado de configurar la **Dirección IP estática**, presione el botón central para continuar.
 - b** Establezca la máscara de subred y luego presione el botón central.
 - c** Establezca la puerta de enlace y luego presione el botón central.
-
- a** Seleccione si desea **Activar** o **Desactivar** el canal de LAN de IPMI. Presione el botón central para continuar.
 - b** En la pantalla **Configuración del iDRAC**, seleccione el icono **Aceptar/Sí** y presione el botón central para aplicar toda la configuración de red de iDRAC a los servidores instalados. Para no aplicar los ajustes de red de la iDRAC a los servidores instalados, seleccione el icono **No** y oprima el botón central y continúe con el paso 3.
 - c** En la siguiente pantalla **Configuración del iDRAC**, seleccione el icono **Aceptar/Sí** y presione el botón central para aplicar toda la configuración de red de iDRAC a los servidores recién instalados; cuando se inserte un servidor nuevo en el chasis, el LCD solicitará al usuario iniciar automáticamente o no el servidor usando los valores/las políticas de red configurados previamente. Para no aplicar la configuración de red de 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 de iDRAC.

- 12 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.
- 13 En la pantalla **Resumen de IP**, revise las direcciones IP que proporcionó para asegurarse de que son correctas. Para corregir un valor, vaya al botón de flecha hacia la izquierda y luego 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 luego presione la tecla central para regresar a la pantalla **Resumen de IP**.

Una vez que haya confirmado que los valores que introdujo son correctos, presione el botón central. El asistente de configuración se cierra y regresa a la pantalla **Menú principal**.



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

El CMC y los iDRAC están ahora disponibles en la red. Puede acceder al CMC en la dirección IP asignada por medio de la interfaz web o las interfaces de línea de comando, 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.

Acceso al CMC a través de una red

Una vez que haya configurado los valores de red del CMC, puede acceder al CMC de manera remota por medio de diversas interfaces. En la Tabla 2-1 se enumeran las interfaces que se pueden utilizar para acceder al CMC de forma remota.



NOTA: Como Telnet no ofrece tanta seguridad como las otras interfaces, está desactivado de manera predeterminada. Para activar Telnet puede utilizar la web, SSH o RACADM remoto.

Tabla 2-1. Interfaces del CMC

Interfaz	Descripción
Interfaz de web	<p>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 acceder a ella por medio de la interfaz del NIC desde un explorador de web compatible en la estación de administración.</p> <p>Para obtener una lista de exploradores web compatibles, consulte la sección correspondiente en la <i>Dell System Software Support Matrix</i> en support.dell.com/manuals.</p>
Interfaz de línea de comandos de RACADM remoto	<p>Proporciona acceso remoto al CMC desde una estación de administración por medio de una interfaz de línea de comandos (CLI). RACADM remoto utiliza la opción <code>racadm -r</code> con la dirección IP del CMC para ejecutar comandos en el CMC.</p> <p>Para obtener más información sobre RACADM remoto, ver “Acceso a RACADM de manera remota” en la página 85 y las secciones subsiguientes.</p>
Telnet	<p>Proporciona acceso de la línea de comandos al CMC a través de la red. La interfaz de línea de comandos RACADM y el comando <code>connect</code>, 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.</p> <p>NOTA: Telnet es un protocolo no seguro que transmite todos los datos (incluso las contraseñas) en texto simple. Al transmitir información confidencial, utilice la interfaz SSH.</p>
SSH	<p>Proporciona las mismas capacidades que Telnet mediante una capa de transporte cifrado para tener una mayor seguridad.</p>



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

Puede acceder a las interfaces web del CMC y del iDRAC a través de la interfaz de red del CMC con un explorador web admitido o bien iniciarlas desde Dell Server Administrator o Dell OpenManage IT Assistant.

Para obtener una lista de exploradores web compatibles, consulte la sección correspondiente en la *Dell System Software Support Matrix* en support.dell.com/manuals. Para acceder al CMC a través de un explorador de web admitido, ver “Acceso a la interfaz web del CMC” en la página 115.

Para acceder a la interfaz del CMC mediante Dell Server Administrator, ejecute Server Administrator en la estación de administración. En el árbol de 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 la *Guía del usuario de Dell Server Administrator*.

Para acceder a la línea de comandos del CMC a través de Telnet o SSH, ver “Configuración del CMC para el uso de consolas de línea de comandos” en la página 65.

Para obtener más información sobre RACADM, ver “Uso de la interfaz de línea de comandos de RACADM” en la página 79.

Para obtener información sobre el uso del comando **connect** o **racadm connect** para conectarse a servidores y módulos de E/S, consulte la sección “Conexión a servidores o módulos de E/S con el comando connect” en la página 71.

Instalación o actualización del firmware de la CMC


En la sección siguiente se describe cómo instalar o actualizar el firmware del CMC.


Descarga del firmware de la CMC


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

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

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

 **NOTA:** Durante las actualizaciones del firmware del CMC, es normal que algunas o todas las unidades de ventilador del chasis giren al 100%.

 **NOTA:** De manera predeterminada, la actualización del firmware retendrá la configuración actual de la CMC. Durante el proceso de actualización, tiene la posibilidad de restablecer los valores predeterminados de fábrica de la CMC.

 **NOTA:** Si tiene CMC redundantes instalados en el chasis, es importante actualizar ambos con la misma versión de firmware. Si los CMC tienen versiones de firmware distintas y se produce una cesión de funciones ante fallas, podrían ocurrir resultados inesperados.

Puede usar el comando **getsysinfo** de RACADM (consulte la sección correspondiente al comando **getsysinfo** en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* [Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC]) o la página **Resumen del chasis** (ver “Cómo ver las versiones actuales del firmware” en la página 213) para ver las versiones actuales de firmware para los CMC instalados en el chasis.

Si tiene un CMC en espera, se recomienda actualizar ambos CMC al mismo tiempo con una sola operación. Cuando el CMC en espera se haya actualizado, intercambie las funciones de los CMC, de manera que el CMC recién actualizado se convierta en el CMC activo y el CMC con el firmware más antiguo se convierta en el CMC en espera. (Consulte la sección correspondiente al comando **cmchangeover** en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) para obtener ayuda sobre el intercambio de funciones). Esto permite verificar que la actualización se realizó correctamente y que el nuevo firmware funciona de forma adecuada antes de actualizar el firmware en el segundo CMC. Cuando ambos CMC se hayan actualizado, se podrá utilizar el comando **cmchangeover** para restaurar los CMC a sus funciones anteriores. La revisión 2.x del firmware de CMC actualiza el CMC principal y el CMC redundante sin utilizar el comando **cmchangeover**.

Actualización del firmware del CMC por medio de la interfaz web

Para obtener instrucciones sobre el uso de la interfaz web para actualizar el firmware del CMC, ver “Actualización de firmware del CMC” en la página 214.


Actualización del firmware del CMC mediante RADCAM

Para obtener instrucciones acerca de cómo utilizar el subcomando `fwupdate` de RACADM para actualizar el firmware del CMC, consulte la sección del comando `fwupdate` en la *Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC*.

Configuración de las propiedades del CMC

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

Para obtener más información acerca de cómo usar la interfaz web, ver “Acceso a la interfaz web del CMC” en la página 115. Para obtener más información sobre el uso de RACADM, ver “Uso de la interfaz de línea de comandos de RACADM” en la página 79.

 **PRECAUCIÓN: Si utiliza más de una herramienta de configuración del CMC al mismo tiempo, podría obtener resultados inesperados.**

Configuración del presupuesto de alimentación

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.

Para obtener más información acerca de la administración de la alimentación en el CMC, ver “Administración de la alimentación” en la página 333.

Para obtener instrucciones acerca de cómo configurar el presupuesto de alimentación y otros valores de la alimentación usando la interfaz web, ver “Configuración del presupuesto de alimentación” en la página 211.

Cómo establecer la configuración de red del CMC



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

Puede configurar los valores de red del CMC con una de las siguientes herramientas:

- RACADM: Para obtener más información, ver “Configuración de múltiples CMC en varios chasis” en la página 104.



NOTA: Si va a implementar el CMC en un entorno de Linux, ver “Instalación de RACADM en una estación de administración con Linux” en la página 41.

- Interfaz web: Para obtener más información, ver “Configuración de las propiedades de red del CMC” en la página 162.

Cómo agregar y configurar usuarios

Puede agregar y configurar usuarios del CMC por medio de RACADM o la interfaz web del CMC. También puede utilizar Microsoft Active Directory para administrar usuarios.

Para obtener instrucciones sobre cómo agregar y configurar usuarios de claves públicas para el CMC por medio de RACADM, ver “Uso de RACADM para configurar la autenticación de claves públicas mediante SSH” en la página 99. Para obtener instrucciones sobre cómo agregar o configurar usuarios a través de la interfaz web, ver “Cómo agregar y configurar usuarios del CMC” en la página 172.

Para obtener instrucciones sobre cómo usar Active Directory con el CMC, ver “Uso del servicio de directorio del CMC” en la página 281.

Cómo agregar alertas de SNMP y por correo electrónico

Puede configurar el CMC para generar alertas de SNMP o por correo electrónico cuando ocurren determinados sucesos del chasis. Para obtener más información, ver “Cómo configurar alertas SNMP” en la página 434 y “Configuración de alertas por correo electrónico” en la página 441.

Configuración de syslog remoto

La función *syslog remoto* se activa y se configura mediante la interfaz gráfica de usuario del CMC o el comando **racadm**. Las opciones de configuración incluyen el nombre del servidor syslog (o dirección IP) y el puerto UDP que utiliza el CMC al reenviar las anotaciones del registro. Se pueden especificar hasta 3 destinos de servidor syslog distintos en la configuración. El syslog remoto es un destino de registro adicional para el CMC. Después de configurar el syslog remoto, cada nueva anotación en el registro generada por CMC se reenvía al destino o los destinos.



NOTA: Puesto que el transporte de red para las anotaciones del registro reenviadas es UDP, no hay garantía de entrega de las anotaciones del registro ni respuestas enviadas al CMC para indicar si se recibieron correctamente.

Para configurar los servicios del CMC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en la ficha **Red**.
- 3 Haga clic en la subficha **Servicios**. Aparecerá la página **Servicios**.

Para obtener más información sobre la configuración del syslog remoto, ver Tabla 5-58.

Descripción del entorno de CMC redundante

Puede 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 plena redundancia y un óptimo rendimiento.

Las protecciones contra fallas pueden ocurrir cuando usted:

- Ejecuta el comando **cmchangeover** de RACADM. (Consulte la sección del comando **cmchangeover** en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC))
- Ejecuta el comando **racreset** de RACADM en el CMC activo. (Consulte la sección del comando **racreset** en la *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 las **Operaciones de control de alimentación** que se describen en “Ejecución de operaciones de control de alimentación en el chasis” en la página 377.)
- 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 del 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.

Acerca del CMC en espera

El CMC en espera es idéntico y se mantiene como un duplicado del CMC activo. Los CMC activo y en espera deben tener instalada la misma revisión del firmware. Si las revisiones del firmware son diferentes, el sistema informará que hay redundancia degradada.

El CMC en espera asume la misma configuración y propiedades del CMC activo. Debe mantener la misma versión del 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, ver el *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 “Instalación o actualización del firmware de la CMC” en la página 56.

Modo a prueba de fallas de CMC

En el modo a prueba de fallas, similar a la protección contra fallas que ofrece el CMC redundante, el gabinete M1000e activa el modo a prueba de fallas para proteger las blade y los módulos de E/S contra fallas. El modo a prueba de fallas se activa cuando no hay ningún CMC controlando el chasis. Durante la protección contra fallas del CMC o durante la pérdida de administración de un CMC:

- Las blade recién instaladas no se pueden activar.
- No es posible acceder a las blade existentes de forma 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 del CMC:

- Extracción del CMC: la administración del chasis se reanuda después de colocar el CMC, o después de la protección contra fallas en el CMC en espera.
- Extracción del cable de red del CMC o pérdida de conexión a la red: la administración del chasis se reanuda cuando el chasis cede el control al CMC en espera después de una falla. La protección contra fallas de la red solo está activa en el modo de CMC redundante.
- Restablecimiento del CMC: la administración del chasis se reanuda después del reinicio del CMC o cuando el chasis cede el control al CMC en espera después de una falla.
- Comando de protección contra fallas del CMC emitido: la administración del chasis se reanuda cuando 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 del reinicio del CMC o cuando el chasis cede el control al CMC en espera después de una falla. Se recomienda actualizar primero el CMC en espera, de manera que solo haya un suceso de protección contra fallas.
- Detección y corrección de errores del CMC: la administración del chasis se reanuda después del reinicio del CMC o cuando el chasis cede el control al CMC en espera después de una falla.



NOTA: El gabinete se puede configurar con un solo CMC o con CMC redundantes. En las configuraciones de CMC redundantes, si el primer CMC pierde la comunicación con el gabinete o la red de administración, el CMC en espera se hace cargo de 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 jerarquía. En vez de ello, 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 la negociación termina.

Obtención del estado de la condición del CMC redundante

Puede ver el estado de la condición del CMC en espera en la interfaz web. Para obtener más información sobre el acceso al estado de la condición del CMC en la interfaz web, ver “Cómo ver los resúmenes del chasis y los componentes” en la página 137.

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

Esta sección 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 explica cómo configurar el sistema para poder ejecutar acciones de administración de sistemas a través de la consola. Para obtener información sobre el uso de los comandos de RACADM en el CMC a través de la consola de línea de comandos, ver “Uso de la interfaz de línea de comandos de RACADM” en la página 79.

Funciones de la consola de línea de comandos en el 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 de RACADM.
- Comando **connect** integrado que se conecta a la consola serie de servidores y a los módulos de E/S; también disponibles como **racadm connect**.
- Historial y edición de línea de comandos.
- Control del tiempo de espera de las sesiones en todas las interfaces de consola.

Uso de una consola Serie, Telnet, o SSH

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

Tabla 3-1. Comandos para la línea de comandos del CMC

Comando	Descripción
racadm	Los comandos RACADM comienzan con la palabra clave racadm seguida de un subcomando, por ejemplo, getconfig , serveraction o getsensorinfo . Ver “Uso de la interfaz de línea de comandos de RACADM” en la página 79 para obtener información sobre el uso de RACADM.
connect	Se conecta a la consola serie de un servidor o módulo de E/S. Ver “Conexión a servidores o módulos de E/S con el comando connect” en la página 71 para obtener ayuda acerca de cómo utilizar el comando connect . NOTA: También se puede utilizar el comando racadm connect .
exit, logout, y quit	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


Se pueden conectar hasta cuatro sistemas cliente Telnet y cuatro clientes SSH en un momento dado.

Si la estación de administración ejecuta Windows XP o Windows 2003, pueden presentarse problemas con caracteres en una sesión Telnet del CMC. El problema puede consistir en un inicio de sesión bloqueado en el que la tecla <Intro> no responde y no aparece el indicador para introducir la contraseña.


Para resolver este problema, descargue la revisión (hotfix) 824810 del sitio web de asistencia de Microsoft en support.microsoft.com. Consulte el artículo 824810 de Microsoft Knowledge Base para obtener más información.

Uso de SSH con el CMC

SSH es una sesión de línea de comandos que incluye las mismas funciones de una sesión Telnet, pero con negociación de sesiones y cifrado para mejorar la seguridad. El CMC admite la versión 2 de SSH con autenticación 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 procedimiento de inicio de sesión, 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 del fallo.

 **NOTA:** OpenSSH se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. También puede ejecutar OpenSSH con Putty.exe. Si se ejecuta OpenSSH en la petición de comandos de Windows no se obtendrá funcionalidad completa (es decir, algunas teclas no responderán y no se mostrarán gráficos). Para 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. El tiempo de espera de la sesión lo controla la propiedad `cfgSsnMgtSshIdleTimeout`. Para obtener más información, consulte el capítulo sobre propiedades de la base de datos de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC), la página de **Administración de servicios** de la interfaz web o consulte “Configuración de servicios” en la página 202.

El CMC también admite autenticación de clave pública (PKA) sobre SSH. Este método de autenticación mejora la automatización de secuencia de comandos de SSH gracias a que evita la necesidad de incorporar o solicitar la identificación/contraseña del usuario. Para obtener más información, ver “Uso de RACADM para configurar la autenticación de claves públicas mediante SSH” en la página 99.

Activación de SSH en el CMC

SSH está activado de manera predeterminada. Cuando SSH está desactivado, puede activarlo por medio de cualquier otra interfaz admitida.

Para obtener instrucciones sobre la activación de conexiones SSH en el CMC mediante RACADM, consulte la sección correspondiente al comando `config` y la sección sobre propiedades de la base de datos `cfgSerial` en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea RACADM de comandos de iDRAC6 y CMC). Para obtener instrucciones sobre la activación de conexiones SSH en el CMC por medio de la interfaz web, ver “Configuración de servicios” en la página 202.

Cambio del puerto de SSH

Para cambiar el puerto SSH, utilice el siguiente comando:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort  
<número de puerto>
```

Para obtener más información sobre las propiedades de `cfgSerialSshEnable` y `cfgRacTuneSshPort`, consulte el capítulo de propiedad de base de datos de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

La implementación de SSH del CMC admite varios esquemas de cifrado, según se muestra en la Tabla 3-2.

Tabla 3-2. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS de 512–1024 bits (aleatorio) según la especificación NIST
Criptografía simétrica	<ul style="list-style-type: none">• AES256-CBC• RIJNDAEL256-CBC• AES192-CBC• RIJNDAEL192-CBC• AES128-CBC• RIJNDAEL128-CBC• BLOWFISH-128-CBC• 3DES-192-CBC• ARCFOUR-128
Integridad del mensaje	<ul style="list-style-type: none">• HMAC-SHA1-160• HMAC-SHA1-96• HMAC-MD5-128• HMAC-MD5-96
Autenticación	Contraseña

Activación del panel anterior para la conexión del iKVM

Para obtener información e instrucciones sobre el uso de los puertos del panel anterior de iKVM, ver “Activación o desactivación del panel anterior” en la página 406.

Configuración del software de emulación de terminal

El CMC admite una consola de texto serie de una estación de administración que ejecute 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 del 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. Consulte la información en “Valores de Minicom requeridos” en la página 70 para configurar otras versiones de Minicom.

Configuración de Minicom versión 2.0



NOTA: Para obtener los mejores resultados, establezca la propiedad `cfgSerialConsoleColumns` para que coincida con el número de columnas. Tenga en cuenta que la petición utiliza dos caracteres. Por ejemplo: para una ventana de terminal de 80 columnas, escriba:

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

- 1 Si no tiene un archivo de configuración de Minicom, vaya al siguiente paso. Si tiene un archivo de configuración Minicom, escriba `minicom <Nombre de archivo de config de Minicom>` y prosiga con paso 13.
- 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 serie adecuado (por ejemplo, `/dev/ttyS0`).

- 5 Presione <e> y defina la opción **Bps/Par/Bits** con el valor **115200 8N1**.
- 6 Presione <f> y luego defina la opción **Control de flujo de hardware** como **Sí** y la opción **Control de flujo de software** como **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 <Retrosceso> para borrar los valores **init**, **reset**, **connect** y **hangup** de modo que queden en blanco y 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 **Guardar configuración como nombre_de_config** y presione <Intro>.
- 11 Seleccione **Salir de Minicom** y presione <Intro>.
- 12 En la petición de shell de comandos, escriba `minicom`
<nombre de archivo de config de Minicom>.
- 13 Presione <Ctrl+a>, <x>, <Intro> para salir de Minicom.

Asegúrese que la ventana de Minicom muestre una petición de inicio de sesión. Cuando la petición de inicio de sesión aparezca, la conexión se habrá establecido satisfactoriamente. Ya está listo para iniciar sesión y acceder la interfaz de línea de comandos del CMC.

Valores de Minicom requeridos

Ver Tabla 3-3 para configurar cualquier versión de Minicom.

Tabla 3-3. Configuración de Minicom

Descripción del valor	Valor necesario
Bps/Par/Bits	115200 8N1
Control de flujo de hardware	Sí
Control de flujo de software	No
Emulación de terminal	ANSI
Marcación de módem y configuración de parámetros	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 de varias maneras:

- Por medio de la línea de comandos del CMC y el comando **connect** o **racadm connect**. Para obtener más información acerca de **connect**, consulte el comando **racadm connect** en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).
- Por medio de la función de redirección de consola serie de la interfaz web del iDRAC.
- Mediante la función de comunicación en serie en LAN (SOL) del iDRAC.

Mientras se encuentra en una consola serie/Telnet/SSH, el CMC admite el comando **connect** para establecer una conexión serie con módulos de E/S y de servidor. La consola serie del servidor contiene el inicio del BIOS y las pantallas de configuración, así como la consola serie del sistema operativo. Para los módulos de E/S, la consola serie 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). Esta opción 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 el cable serie se quita 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>**.

Existen hasta seis módulos de E/S en el sistema administrado. Para conectarse a un módulo de E/S escriba:


```
connect switch-n
```


en donde *n* es una etiqueta del módulo de E/S A1, A2, B1, B2, C1 y C2.

(Consulte la Ilustración 11-1 para ver una ilustración de la colocación de los módulos de E/S en el chasis.) Cuando 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 3-4.

Tabla 3-4. 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 or switch-6


 **NOTA:** Solo puede haber una conexión de módulo de E/S por chasis al mismo tiempo.

 **NOTA:** No es posible establecer conexiones de paso desde la consola serie.

Para conectarse a una consola serie de servidor administrado, utilice el comando **connect server-n**, en donde *-n* es el número de ranura del servidor; también puede utilizarse 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 iDRAC no se encuentra disponible, aparecerá el mensaje de error **No hay ruta al host**.

El comando **connect server-n** permite al usuario acceder al puerto serie del servidor. Tras establecer la conexión, el usuario podrá ver la redirección de la consola del servidor a través del puerto serie del CMC que incluye la consola serie de BIOS y la consola serie del sistema operativo.

 **NOTA:** Para ver las pantallas de inicio del BIOS, es necesario activar la redirección serie en la configuración del BIOS de los servidores. Además, la ventana del emulador de terminal se debe configurar en 80x25. De modo contrario, la pantalla no podrá leerse.

 **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.

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

Es necesario conectarse al servidor administrado por medio del iKVM (ver “Administración de servidores con iKVM” en la página 394), o establecer una sesión de la consola remota desde la interfaz gráfica de usuario web del iDRAC (consulte la *Guía del usuario del iDRAC* en support.dell.com/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 llegar a **Comunicación serie** y presione <Intro>. En el cuadro de diálogo emergente, la lista de comunicación serie muestra estas opciones:
 - apagado
 - encendido sin redirección de consola
 - encendido con redirección de consola a través de COM1

Utilice las teclas de flecha para recorrer las opciones.


- 4 Asegúrese de que la opción **Encendido con redirección de consola a través de COM1** esté activada.
- 5 Active la opción **Redirección después de inicio** (el valor predeterminado es **desactivada**). Esta opción activa la redirección de consola del BIOS en los reinicios subsiguientes.
- 6 Guarde los cambios y salga.
- 7 El servidor administrado se reinicia.

Configuración de Windows para la redirección de consola 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) en el COM1.

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

Los pasos a continuación son específicos para GRand Unified Bootloader (GRUB) de Linux. Si se utiliza otro cargador de inicio, será necesario hacer cambios similares.

 **NOTA:** Cuando configure la ventana de emulación de cliente VT100, configure 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` como 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 Agregue dos opciones a la línea de núcleo:

```
kernel console=ttyS1,57600
```

- 3 Si el archivo `/etc/grub.conf` contiene una directiva `splashimage`, inserte un carácter de comentario al inicio de la línea para anularla.

El siguiente ejemplo ilustra los cambios descritos en este procedimiento.

```
# grub.conf generado por anaconda
N.º
# Tenga en cuenta que no tiene que volver a ejecutar
grub después de hacer cambios
# en este archivo
# AVISO: Usted no tiene una partición /boot. Esto
significa que
#     todas las rutas de acceso de initrd o
núcleo son relativas a /, p. ej.
#     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 de texto. De lo contrario, la pantalla de GRUB no se mostrará en la redirección de la consola. Para desactivar la interfaz gráfica, inserte un carácter de comentario al inicio de la línea que comienza con `splashimage`.
- Para abrir varias opciones de GRUB a fin de iniciar sesiones de consola por medio de la conexión serie, agregue la siguiente línea a todas las opciones:

```
console=ttyS1,57600
```

El ejemplo muestra el elemento `console=ttyS1,57600` agregado solo a la primera opción.

Configuración de Linux para la redirección de la 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.

```
N.º
# inittab Este archivo describe cómo el proceso de
INIT
#         debe configurar el sistema en un cierto
#         nivel de ejecución.
N.º
# Autor:  Miguel van Smoorenburg
#         Modificado para RHS Linux por Marc Ewing y
#         Donnie Barnes
N.º
# Nivel de ejecución predeterminado. Los niveles de
ejecución que utiliza RHS son:
#  0: Alto (NO establezca initdefault con este valor)
#  1: Modo de un solo usuario
#  2: Varios usuarios, sin NFS (igual que el valor 3,
si no
#     se tiene red)
#  3: Modo completo de varios usuarios
#  4: No se utiliza
#  5: X11
#  6: Reiniciar (NO establezca initdefault con este
valor)
N.º
id:3:initdefault:

# Inicialización del sistema.
si::sysinit:/etc/rc.d/rc.sysinit
```

```
10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

# Cosas que se deben ejecutar en cada nivel de
ejecución.
ud::once:/sbin/update

# Captura CTRL-ALT-SUPRIMIR
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# Cuando nuestra fuente de alimentación ininterrump-
ible informe que la alimentación ha fallado, suponer
que nos quedan unos cuantos
# minutos de alimentación eléctrica restantes. Pro-
gramar un apagado en 2 minutos a partir de este
momento.
# Obviamente, esto supone que se tiene alimentación
instalada y que la
# fuente de alimentación ininterrumpible está
conectada y funciona correctamente.
pf::powerfail:/sbin/shutdown -f -h +2 "Falla de ali-
mentación; el sistema se está apagando"
# Si la alimentación se restaura antes de que el apa-
gado inicie, cancelar el apagado.
pr:12345:powerokwait:/sbin/shutdown -c "Alimentación
restaurada; se canceló el apagado"
```

```
# Ejecutar gettys en los niveles de ejecución
estándares
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
```

```
# Ejecutar xdm en el nivel de ejecución 5
# xdm ahora es un servicio separado
x:5:respawn:/etc/X11/prefdm -nodaemonModifique 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
```

Uso de la interfaz de línea de comandos de RACADM

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

La interfaz RACADM se clasifica de la siguiente manera:



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

- RACADM remoto: permite ejecutar comandos de 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 Telnet, SSH, una conexión serie o el iKVM. Con RACADM de firmware se ejecuta la implementación de RACADM que es parte del firmware del CMC.

Puede utilizar comandos de RACADM remoto en secuencias de comandos para configurar varios CMC. El CMC no admite secuencias de comandos, por lo que no puede ejecutar secuencias de comandos directamente en el CMC. Para obtener más información acerca de cómo configurar varios CMC, ver “Configuración de múltiples CMC en varios chasis” en la página 104.

Uso de una consola Serie, Telnet, o SSH

Puede iniciar sesión en el CMC mediante una conexión serie o Telnet/SSH, o por medio de la consola del CMC de Dell en el iKVM. Para configurar el CMC para el acceso serie o remoto, ver “Configuración del CMC para el uso de consolas de línea de comandos” en la página 65. Las opciones de subcomandos de uso más frecuente se muestran en la Tabla 4-2. En el capítulo de subcomandos de RACADM de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) hay una lista completa de subcomandos RACADM.

Inicio de sesión en el CMC

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

- 1 Conéctese al 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 después presione <Intro>.

Ahora está conectado al CMC.

Inicio de una consola de texto

Puede iniciar sesión en el CMC mediante Telnet o SSH a través de una red, un puerto serie o una consola del CMC de Dell por medio del iKVM. Abra una sesión de Telnet o SSH, conéctese e inicie sesión en el CMC.

Para obtener información acerca de cómo conectarse al CMC a través del iKVM, ver “Uso del módulo iKVM” en la página 387.

Cómo utilizar de RACADM

Los subcomandos RACADM se pueden ejecutar de manera remota desde la petición de comandos de la consola serie, Telnet o SSH, o por medio de una petición de comandos normal.

Utilice los subcomandos de RACADM para configurar las propiedades del CMC y realizar tareas de administración de manera remota. Para ver una lista de subcomandos de RACADM, escriba:

```
racadm help
```

Cuando se ejecuta sin opciones ni subcomandos, RACADM muestra información de la sintaxis e instrucciones para acceder a los subcomandos y a la ayuda. Para ver una lista de las opciones de sintaxis y de línea de comandos para subcomandos individuales, escriba:

```
racadm help <subcomando>
```


Subcomandos de RACADM

La Tabla 4-1 proporciona una lista breve de subcomandos comunes que se utilizan en RACADM. Para ver una lista completa de los subcomandos de RACADM, incluidas la sintaxis y las anotaciones válidas, ver el capítulo de subcomandos de RACADM de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).



NOTA: El comando **connect** está disponible como comando RACADM y como comando integrado del CMC. Los comandos **exit**, **quit** y **logout** son comandos integrados del CMC, no comandos de RACADM. Ninguno de ellos se puede utilizar con RACADM remoto. Para obtener información sobre el uso de estos comandos, ver “Conexión a servidores o módulos de E/S con el comando connect” en la página 71.

Tabla 4-1. Subcomandos de RACADM

Comando	Descripción
help	Muestra las descripciones de los subcomandos del CMC.
help <subcomando>	Muestra el resumen sobre el uso del subcomando especificado.
?	Muestra las descripciones de los subcomandos del CMC.
? <subcomando>	Muestra el resumen sobre el uso del subcomando especificado.
arp	Muestra el contenido de la tabla ARP. Las anotaciones de la tabla ARP no se pueden agregar ni eliminar.
chassisaction	Ejecuta el encendido, el apagado, el restablecimiento y el ciclo de encendido en el chasis, el conmutador y el KVM.
closesn	Cierra una sesión.
clrraclog	Borra el registro del CMC y crea una sola anotación que indica el usuario y la hora a la que se borró el registro.
clrsel	Borra las anotaciones del registro de sucesos del sistema.
cmchangeover	Cambia el estado del CMC de activo a modo de espera, o viceversa, en entornos de CMC redundantes.
config	Configura el CMC.
connect	Se conecta a la consola serie de un servidor o módulo de E/S. Ver “Conexión a servidores o módulos de E/S con el comando connect” en la página 71 para obtener ayuda acerca de cómo utilizar el comando connect .

Tabla 4-1. Subcomandos de RACADM (continuación)

Comando	Descripción
deploy	Implementa un servidor mediante la especificación de las propiedades requeridas.
feature	Muestra las funciones activadas y la desactivación de las funciones.
featurecard	Muestra información del estado de la tarjeta de función.
fwupdate	Realiza actualizaciones de firmware de los componentes del sistema, y muestra el estado de actualización del firmware.
getassettag	Muestra la etiqueta de propiedad del chasis.
getchassisname	Muestra el nombre del chasis.
getConfig	Muestra las propiedades de configuración actuales del CMC.
getdcinfo	Muestra información general de configuración errónea del módulo de E/S y de la tarjeta subordinada.
getfanreqinfo	Muestra la solicitud del ventilador para servidores y conmutadores en %.
getflexaddr	Muestra el estado activado/desactivado de FlexAddress por ranura/red Fabric Si se utiliza la opción -i , el comando muestra las direcciones WWN y MAC para una ranura en particular.
getioinfo	Muestra información general del módulo de E/S.
getkvminfo	Muestra información acerca del iKVM.
getled	Muestra la configuración de los LED en un módulo.
getmacaddress	Muestra la dirección MAC de un servidor.
getmodinfo	Muestra información de la configuración del módulo y del estado.
getniccfg	Muestra la configuración IP actual para la controladora.
getpbinfo	Muestra información del estado del presupuesto de alimentación.
getpminfo	Muestra información del estado de la administración de alimentación.
getraclog	Muestra el registro del CMC.
getractime	Muestra la hora del CMC.
getredundancymode	Muestra el modo de redundancia del CMC.

Tabla 4-1. Subcomandos de RACADM (continuación)

Comando	Descripción
getsel	Muestra el registro de sucesos del sistema (registro de hardware).
getsensorinfo	Muestra información acerca de los sensores del sistema.
getslotname	Muestra el nombre de una ranura en el chasis.
getssninfo	Muestra información sobre las sesiones activas.
getsvctag	Muestra las etiquetas de servicio.
getsysinfo	Muestra información general del CMC y del sistema.
gettracelog	Muestra el registro de rastreo del CMC. Si se utiliza con la opción -i , el comando muestra el número de anotaciones en el registro de rastreo del CMC.
getversion	Muestra la versión de software actual, la información de modelo, y si se puede actualizar o no el dispositivo.
ifconfig	Muestra la configuración actual de IP del CMC.
krbkeytabupload	Carga un archivo keytab de Kerberos en el CMC.
netstat	Muestra la tabla de enrutamiento y las conexiones actuales.
ping	Verifica que se pueda acceder a la dirección IPv4 de destino desde el CMC con el contenido actual de la tabla de enrutamiento.
ping6	Verifica que se pueda acceder a la dirección IPv6 de destino desde el CMC con el contenido actual de la tabla de enrutamiento.
racdump	Muestra información completa del estado de configuración y del estado del chasis, así como también registros de historial de sucesos. Se utiliza para realizar una verificación de la configuración después de la implementación y durante las sesiones de depuración de errores.
racreset	Restablece el CMC.
racresetcfg	Restablece la configuración predeterminada del CMC.
remoteimage	Conecta, desconecta o implementa un archivo de soportes en un servidor remoto.
serveraction	Realiza operaciones de administración de la alimentación en el sistema administrado.
setassettag	Establece la etiqueta de propiedad del chasis.

Tabla 4-1. Subcomandos de RACADM (continuación)

Comando	Descripción
setchassisname	Establece el nombre del chasis.
setflexaddr	Activa/desactiva FlexAddress en una ranura/red Fabric particular, cuando la función FlexAddress está activada en el chasis.
setled	Establece la configuración de los indicadores LED de un módulo.
setniccfg	Establece la configuración IP de la controladora.
setractime	Establece la hora del CMC.
setslotname	Establece el nombre de una ranura en el chasis.
setsysinfo	Establece el nombre y la ubicación del chasis.
sshpkauth	Carga hasta seis claves públicas de SSH diferentes, elimina las claves existentes y muestra las que ya se utilizan en el CMC.
sslcertdownload	Descarga un certificado firmado por una autoridad de certificados.
sslcertupload	Carga un certificado firmado por una autoridad de certificados o un certificado de servidor en el CMC.
sslcertview	Muestra un certificado firmado por una autoridad de certificados o un certificado de servidor en el CMC.
sslcsrgen	Genera y descarga la CSR de SSL.
sslresetcfg	Genera nuevamente el certificado autofirmado que utiliza la interfaz gráfica de usuario web del CMC.
testemail	Obliga al CMC a enviar un correo electrónico a través del NIC del CMC.
testfeature	Permite verificar los parámetros de configuración de una función específica. Por ejemplo: Admite la prueba de la configuración de Active Directory mediante la autenticación simple (nombre de usuario y contraseña) o la configuración de Active Directory con la autenticación de Kerberos (inicio de sesión único o inicio de sesión mediante tarjeta inteligente).
testtrap	Obliga al CMC a enviar un SNMP a través de la interfaz de red del CMC.
traceroute	Imprime la ruta que los paquetes IPv4 toman a un nodo de red.
traceroute6	Imprime la ruta que los paquetes IPv6 toman a un nodo de red.

Acceso a RACADM de manera remota

Tabla 4-2. Opciones de los subcomandos de RACADM remoto

Opción	Descripción
-r <racIpAddr>	Especifica la dirección IP remota de la controladora.
-r <racIpAddr>:<puerto>	Utilice <número de puerto> si el número de puerto del CMC no es el puerto predeterminado (443).
-i	Indica a RACADM que solicite interactivamente al usuario el nombre de usuario y la contraseña.
-u <usrName>	Especifica el nombre de usuario que se usa para autenticar la transacción del comando. Si se utiliza la opción -u , se debe utilizar la opción -p , y la opción -i (interactiva) no se permite.
-p <contraseña>	Especifica la contraseña usada para autenticar la transacción del comando. Si se utiliza la opción -p , la opción -i no se permite.

Para acceder a RACADM de manera remota, escriba los siguientes comandos:

```
racadm -r <dirección IP de CMC> -u <nombre_de_usuario>
-p <contraseña> <subcomando> <opciones de subcomando>
racadm -i -r <dirección IP de CMC> <subcomando>
<opciones de subcomando>
```



NOTA: La opción **-i** indica a RACADM que solicite interactivamente el nombre de usuario y la contraseña. Sin la opción **-i**, usted debe proporcionar el nombre de usuario y la contraseña en el comando mediante las opciones **-u** y **-p**.

Por ejemplo:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
racadm -i -r 192.168.0.120 getsysinfo
```

Si el número de puerto HTTPS del CMC se ha cambiado a un puerto personalizado distinto del puerto predeterminado (443), se debe utilizar la siguiente sintaxis:

```
racadm -r <dirección IP de CMC>:<puerto> -u  
<nombre_de_usuario> -p <contraseña> <subcomando>  
<opciones de subcomando>
```

```
racadm -i -r <dirección IP de CMC>:<puerto>  
<subcomando> <opciones de subcomando>
```

Activación y desactivación de la capacidad remota de RACADM



NOTA: Dell recomienda ejecutar estos comandos en el chasis.

La capacidad remota de RACADM en el CMC está activada de manera predeterminada. En los siguientes comandos, **g** especifica el grupo de configuración al que pertenece el objeto y **-o** especifica el objeto de configuración que se va a configurar.

Para desactivar la capacidad remota de RACADM, escriba:

```
racadm config -g cfgRacTuning -o  
cfgRacTuneRemoteRacadmEnable 0
```

Para volver a activar la capacidad remota de RACADM, escriba:

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

Uso de RACADM de manera remota



NOTA: Configure la dirección IP en el CMC antes de utilizar la capacidad remota de RACADM. Para obtener más información acerca de cómo configurar el CMC, ver “Instalación y configuración del CMC” en la página 35.


La opción remota (**-r**) de la consola de RACADM le permite conectarse al sistema administrado y ejecutar subcomandos de RACADM desde una consola remota o una estación de administración. Para utilizar la capacidad remota, se necesita un nombre de usuario válido (opción **-u**), una contraseña (opción **-p**) y la dirección IP del CMC.


Antes de intentar acceder a RACADM de manera remota, confirme que tiene los permisos para hacerlo. Para ver sus privilegios de usuario, escriba:

```
racadm getconfig -g cfguseradmin -i n
```

donde *n* es su identificación de usuario (de 1 a 16).

Si no conoce su identificación de usuario, intente utilizar distintos valores para *n*.

 **NOTA:** La capacidad remota de RACADM se admite solo en estaciones de administración mediante un explorador admitido. Para obtener más información, consulte la sección Exploradores admitidos en la *Dell Systems Software Support Matrix* en support.dell.com/manuals.

 **NOTA:** Cuando se utiliza la capacidad remota de RACADM, se debe tener permiso de escritura en las carpetas donde se van a utilizar los subcomandos de RACADM que involucren operaciones con archivos. Por ejemplo:

```
racadm getconfig -f <nombre de archivo> -r
<dirección IP>
or
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Cuando se utiliza RACADM remoto para capturar los grupos de configuración en un archivo, si no se define una propiedad clave dentro del grupo, el grupo de configuración no se guardará como parte del archivo de configuración. Si es necesario clonar estos grupos de configuración en otros CMC, se debe definir la propiedad clave antes de ejecutar el comando `getconfig -f`. También se pueden introducir manualmente las propiedades faltantes en el archivo de configuración después de ejecutar el comando `getconfig -f`. Esto se aplica a todos los grupos indexados de `racadm`.


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

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

Mensajes de error de RACADM

Para obtener información acerca de los mensajes de error de la CLI de RACADM, ver “Solución de problemas” en la página 112.

Uso de RACADM para configurar el CMC

 **NOTA:** Antes de configurar el CMC por primera vez, deberá iniciar sesión como usuario raíz para ejecutar comandos RACADM en un sistema remoto. Se puede crear otro usuario con privilegios para configurar el CMC.

La interfaz web del CMC es la forma más rápida de configurar el CMC (ver “Uso de la interfaz web del CMC” en la página 115). Sin embargo, si prefiere la configuración mediante CLI o secuencia de comandos, o si necesita configurar varios CMC, utilice RACADM remoto, que se instala con los agentes del CMC

en la estación de administración.

Configuración de las propiedades de red del CMC

Antes de que pueda comenzar a configurar el CMC, debe configurar primero los valores de red del CMC para permitir la administración del CMC de manera remota. Esta configuración inicial asigna los parámetros del sistema de red TCP/IP que permiten tener acceso al CMC.

Configuración del acceso inicial al CMC

En esta sección se explica cómo realizar la configuración inicial de red del CMC por medio de los comandos de RACADM. Toda la configuración descrita en esta sección se puede realizar por medio de la pantalla LCD del panel anterior. Vea la “Configuración del sistema de red por medio del asistente de configuración del panel LCD” en la página 48.

 **PRECAUCIÓN:** Si cambia la configuración en la pantalla Configuración de red del CMC podría desconectar su conexión de red actual.

Para obtener más información acerca de los subcomandos de red, consulte los capítulos sobre subcomandos de RACADM y definiciones de grupos y objetos de bases de datos de propiedades de la *Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC*.



NOTA: Debe tener privilegios de Administrador de configuración del chasis para definir la configuración de la red del CMC.

El CMC es compatible con los modos de direccionamiento IPv4 e IPv6. Los valores de configuración de IPv4 e IPv6 son totalmente independientes.

Cómo ver la configuración de la red actual de IPv4

Para ver un resumen de la configuración del NIC, el DHCP, la velocidad de la red y dúplex, escriba:

```
racadm getniccfg
```

o

```
racadm getconfig -g cfgCurrentLanNetworking
```

Cómo ver la configuración de la red actual de IPv6

Para ver un resumen de la configuración de la red, escriba:

```
racadm getconfig -g cfgIpv6LanNetworking
```


Para ver la información de direccionamiento de IPv4 e IPv6 para el chasis, escriba:

```
racadm getsysinfo
```

De manera predeterminada, el CMC solicita y obtiene automáticamente una dirección IP del CMC a partir del servidor de protocolo de configuración dinámica de host (DHCP).

Puede desactivar esta función y especificar la dirección IP estática del CMC, la puerta de enlace y la máscara de subred.

Para desactivar el DHCP y especificar la dirección IP estática del CMC, la puerta de enlace y la máscara de subred, 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>
```

Cómo ver la configuración de red actual

Para ver un resumen de la configuración del NIC, el DHCP, la velocidad de la red y dúplex, escriba:

```
racadm getniccfg
```

```
o
```

```
racadm getconfig -g cfgCurrentLanNetworking
```

Para ver la dirección IP y DHCP, la dirección MAC y la información de DNS del chasis, escriba:

```
racadm getsysinfo
```


Configuración de los valores de red de la LAN




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



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


 **NOTA:** Si se tienen dos CMC (activo y en espera) en el chasis y están conectados a la red, el CMC en espera asumirá automáticamente la configuración de la red en caso que el CMC activo falle.

 **NOTA:** 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 conmutadores externos queden bloqueados durante un plazo mayor a los doce segundos en los que se envían las solicitudes de enrutador IPv6. En tales casos, puede haber un período en el que la conectividad de IPv6 sea limitada, hasta que los anuncios del enrutador sean enviados por los enrutadores IPv6 sin ser requeridos.

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 manera 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 del CMC a partir del servidor de protocolo de configuración dinámica de host (DHCP). La función de DHCP se puede desactivar y se puede especificar la dirección IP, la 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>
```

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 está activada, la función de DHCP para la dirección del 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 manera predeterminada.

Se puede desactivar la función de DHCP para la dirección del NIC y especificar dirección IP, máscara de subred y puerta de enlace estáticas. Para obtener más información, consulte “Configuración del acceso inicial al CMC” en la página 88.

Activación o desactivación del DHCP para la dirección IP de DNS

De manera predeterminada, la función de DHCP para la dirección de DNS del CMC está desactivada. Cuando está activada, esta función obtiene las direcciones de los servidores DNS principal y secundario a partir del servidor DHCP. Mientras utiliza esta función, no tiene que configurar direcciones IP estáticas para el servidor DNS.

Para desactivar la función de 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 de 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
```

Cómo establecer direcciones IP estáticas de DNS



NOTA: La configuración de direcciones IP estáticas de DNS solo será válida cuando la función de DHCP para la dirección de DNS esté 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-IP>
```

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 de los servidores DNS solo registran nombres de 31 caracteres o menos. Asegúrese de que el nombre designado esté dentro del 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 del dominio DNS.** El nombre predeterminado del dominio DNS es un solo carácter en blanco. Para establecer un nombre de dominio DNS, escriba:

```
racadm config -g cfgLanNetworking -o cfgDNSDomainName <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 está activada, la función de negociación automática determina si el CMC establece automáticamente el modo dúplex y la velocidad de la red al comunicarse con el enrutador o el conmutador más cercano. La negociación automática está activada de manera predeterminada.

Se podrá 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 ó 100 (valor predeterminado).

Configuración de la VLAN del CMC (IPv4 e IPv6)

- 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 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
```

Eliminación de la VLAN del CMC

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 VLAN de un servidor

Especifique la identificación y la prioridad de VLAN de un servidor específico con el siguiente comando:

```
racadm setniccfg -m server-<n> -v <id de VLAN> <VLAN  
priority>
```

Los valores válidos para <n> son de 1 a 16.

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

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

Por ejemplo:

```
racadm setniccfg -m server-1 -v 1 7
```

Eliminación de VLAN de un servidor

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

La propiedad MTU le permite establecer un límite para el paquete más grande que se puede pasar a través de la interfaz. Para establecer 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` tiene un valor menor, el CMC utilizará una MTU de 1280.

Configuración de la dirección IP del servidor SMTP (IPv4 e IPv6)

Usted puede activar el CMC para enviar alertas por correo electrónico con el protocolo simple de transferencia de correo (SMTP) a una dirección IP específica. Para activar esta función, escriba:

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSmtplibServerIpAddr <dirección IP de SMTP>
```

donde <dirección IP de SMTP> es la dirección IP del servidor SMTP de la red.



NOTA: 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 periodo durante el cual el valor de esta propiedad no funcionará debido al cambio en la dirección IP especificada del servidor SMTP. En estos casos, utilice el nombre DNS.

Configuración de los valores de seguridad de la red (solo IPv4)

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

Activación de la comprobación de rango de IP (solo IPv4)

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP que se especifica en las siguientes propiedades de `cfgRacTuning`:

- `cfgRacTuneIpRangeAddr`
- `cfgRacTuneIpRangeMask`

Solo se autoriza un inicio de sesión de una dirección IP entrante si los valores siguientes son idénticos:

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

Uso de RACADM para configurar usuarios

Puede configurar hasta 16 usuarios en la base de datos de propiedades del CMC. Antes de activar manualmente a un usuario del CMC, verifique si existe algún usuario actual. Si está configurando un nuevo CMC o ejecutó el comando `racresetcfg` de RACADM, el único usuario actual es `raíz` con la contraseña `calvin`. El subcomando `racresetcfg` restablece al CMC a sus valores predeterminados originales.



PRECAUCIÓN: Tenga precaución cuando utilice el comando `racresetcfg` ya que restablecerá *todos* los parámetros de configuración originales. Todos los cambios anteriores se perderán.



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 <índice>
```

Se muestran varios parámetros e identificaciones de objetos con sus valores actuales. Los dos objetos de interés son:

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

Si el objeto `cfgUserAdminUserName` no tiene un valor, el número de índice que indica el objeto `cfgUserAdminIndex` está disponible para su uso. Si hay un nombre después del signo “=”, el nombre de usuario tomará ese índice.



NOTA: Cuando activa o desactiva un usuario manualmente con el subcomando `config` de RACADM, *es necesario* especificar el índice con la opción `-i`. Note que el objeto `cfgUserAdminIndex` que se muestra en el ejemplo anterior contiene un carácter #. Además, si se utiliza el comando `racadm config -f racadm.cfg` para especificar el número de grupos/objetos por escribir, el índice no se podrá especificar. Se agrega un nuevo usuario al primer índice disponible. Este comportamiento permite tener más flexibilidad al configurar un segundo CMC con los mismos valores que los del CMC principal.

Cómo agregar un usuario del CMC

Para agregar un nuevo usuario a la configuración del CMC, se pueden utilizar unos cuantos comandos básicos. Realice los procedimientos siguientes:

- 1 Establezca el nombre de usuario.
- 2 Establezca la contraseña.
- 3 Establezca los privilegios de usuario. Para obtener información sobre privilegios de usuario, consulte las secciones Tabla 5-42 y Tabla 5-43.
- 4 Active el usuario.

Ejemplo

El siguiente ejemplo describe cómo agregar un nuevo usuario denominado “Juan” con la contraseña “123456” y privilegios de inicio de sesión en el CMC.



NOTA: Consulte la tabla 3-1 en el capítulo de propiedades de la base de datos de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) para ver una lista de los valores de máscara de bits válidos para determinados privilegios de usuario.

El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios activados.

```
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 añadido satisfactoriamente con los privilegios adecuados, escriba el siguiente comando:

```
racadm getconfig -g cfgUserAdmin -i 2
```

Uso de RACADM para configurar la autenticación de claves públicas mediante SSH

Es posible configurar hasta 6 claves públicas que se pueden utilizar con el nombre de usuario “service” mediante 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 de ellas. El nombre de usuario “service” es una cuenta de usuario especial que se puede utilizar para acceder al CMC mediante SSH. Cuando la autenticación de claves públicas mediante SSH está configurada y se utiliza correctamente, no es necesario introducir un nombre de usuario ni contraseñas para iniciar sesión en el CMC. Esta función puede resultar de mucha utilidad para configurar secuencias de comandos automáticas para ejecutar diferentes funciones.

Cuando se prepare para configurar esta función, tenga en cuenta lo siguiente:

- No hay soporte de interfaz gráfica de usuario para administrar esta función; solamente se puede utilizar RACADM.
- Al agregar claves públicas nuevas, verifique que las claves existentes no se encuentren ya en el índice donde se agregará la clave nueva. El CMC no realiza comprobaciones para verificar que las claves anteriores se han eliminado antes de agregar una nueva. Tan pronto se agrega una clave nueva, automáticamente entra en vigor siempre que la interfaz de SSH esté activada.
- Cuando utilice la sección del 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 autenticación de claves públicas utilizan 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
```

Tipo	Usuario	Dirección IP	Fecha y hora de inicio de sesión
SSH 09:00:00	PC1	x.x.x.x	06/16/2009
SSH 09:00:00	PC2	x.x.x.x	06/16/2009

Para obtener más información sobre `sshpkeygen`, consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Generación de claves públicas para Windows

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

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

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

- 1 Inicie la aplicación y seleccione SSH-2 RSA o SSH-2 DSA para el tipo de clave que generará (SSH-1 no es compatible).
- 2 Introduzca el número de bits para la clave. El número debe estar entre 768 y 4096.



NOTA: Es posible que el CMC no muestre un mensaje si agrega claves menores de 768 o mayores de 4.096, pero al intentar iniciar sesión estas claves fallan.

- 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 introducir una frase contraseña para asegurar la clave. Verifique que ha guardado 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 desde la ventana **Clave pública para pegar** al agregar la cuenta mediante la opción de texto

Generación de claves públicas para Linux

La aplicación `ssh-keygen` para clientes Linux es una herramienta de línea de comandos sin interfaz gráfica de usuario. Abra una ventana de terminal y en la petición de shell escriba:

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

donde,

la opción `-t` debe ser `dsa` o `rsa`.

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

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

La <frase de acceso> 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 utiliza 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. El parámetro `svcacct` representa una cuenta especial para la autenticación de la clave pública mediante SSH en CMC.
- Para iniciar sesión en el CMC, el usuario debe ser `service`. Los usuarios de otras categorías tienen acceso a las claves públicas introducidas por medio del comando `sshpkauth`.

Cómo ver las claves públicas

Para ver las claves públicas que se han agregado al CMC, escriba:

```
racadm sshpkauth -i svcacct -k all -v
```

Para ver una sola clave por vez, reemplace `all` con un número de 1 a 6.

Por ejemplo, para ver la clave 2, escriba:

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

Cómo agregar 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 0xffff -f <archivo de clave pública>
```



NOTA: La opción de carga de archivo solo puede utilizarse con RACADM remoto. Para obtener más información, ver “Acceso a RACADM de manera remota” en la página 85 y las secciones subsiguientes.

Para ver los privilegios de clave pública, consulte la tabla 3-1 en el capítulo sobre propiedades de la base de datos de la *Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC*.

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

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -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
```

Inicio de sesión con autenticación de clave pública

Después de cargar las claves públicas, deberá poder iniciar sesión en el CMC mediante SSH sin tener que introducir una contraseña. También tendrá la opción de enviar un solo comando de RACADM como argumento de línea de comandos a la aplicación de SSH. Las opciones de línea de comandos se comportan como RACADM remoto ya que la sesión finaliza al completarse el comando. Por ejemplo:

Conectar:

```
ssh service@<dominio>
```

O bien:

```
ssh service@<dirección_IP>
```

donde `<dirección_IP>` es la dirección IP del CMC.

Envío de comandos racadm:

```
ssh service@<dominio> racadm getversion  
ssh service@<dominio> racadm getsel
```

Si se configuró una frase contraseña al crear el par de claves públicas/privadas, al iniciar sesión con la cuenta “service”, es posible que se le indique que debe volver a introducir la frase contraseña. Si se utiliza una frase 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 contraseña sea imperceptible. Para los clientes Linux se puede utilizar ssh-agent. Para configurar y utilizar cualquiera de estas aplicaciones, consulte la documentación que las acompaña.

Activación de un usuario del CMC con permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en funciones), primero localice un índice de usuario disponible mediante los pasos descritos en “Antes de comenzar” en la página 35. A continuación, escriba las siguientes líneas de comandos con el nuevo nombre de usuario y contraseña:

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



NOTA: Consulte la tabla 3-1 en el capítulo de propiedades de la base de datos de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) para ver una lista de los valores de máscara de bits válidos para determinados privilegios de usuario. El valor de privilegios predeterminado es 0, lo que indica que el usuario no tiene privilegios activados.

Desactivación de un usuario del CMC

Por medio de RACADM, solo es posible desactivar usuarios del CMC manualmente y de forma individual. No es posible eliminar usuarios mediante un archivo de configuración.

El siguiente ejemplo muestra la sintaxis del comando que se puede utilizar para eliminar un usuario del CMC:

```
racadm config -g cfgUserAdmin -i 2  
cfgUserAdminPrivilege 0x0
```

Configuración de alertas de SNMP y por correo electrónico

Usted puede configurar el CMC para enviar capturas de sucesos de SNMP y/o de correo electrónico cuando ocurren ciertos sucesos en el chasis. Para obtener más información e instrucciones, ver “Cómo configurar alertas SNMP” en la página 434 y “Configuración de alertas por correo electrónico” en la página 441.

Es posible especificar destinos de captura como direcciones numéricas (IPv6 o IPv4) con el formato adecuado o nombres de dominio completamente expresados (FQDN). Elija un formato que sea coherente con la tecnología/infraestructura de su sistema de red.



NOTA: La función de **Captura de prueba** no detecta elecciones incorrectas con base en la configuración de red actual. Por ejemplo, si se utiliza un destino IPv6 en un entorno exclusivo de IPv4.

Configuración de múltiples CMC en varios chasis

Por medio de RACADM, usted puede configurar uno o varios CMC con propiedades idénticas.

Cuando 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, usted puede 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 Utilice RACADM para hacer una consulta en el CMC de destino que contiene la configuración deseada.



NOTA: El archivo de configuración generado es **miarchivo.cfg**. Usted puede cambiar el nombre del archivo.



NOTA: El archivo **.cfg** no contiene contraseñas de usuario. Cuando el archivo **.cfg** se carga en el nuevo CMC, 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. Para obtener más información, ver “Acceso a RACADM de manera remota” en la página 85.

- 3 Modifique el archivo de configuración con un editor de textos simple (opcional). Cualquier carácter de formato especial en el archivo de configuración podría dañar la base de datos de RACADM.
- 4 Utilice el archivo de configuración recién creado para modificar un CMC de destino.

En el indicador de comandos, escriba:

```
racadm config -f myfile.cfg
```

- 5 Restablezca el CMC de destino que fue configurado. En el indicador de comandos, escriba:

```
racadm reset
```

El subcomando `getconfig -f miarchivo.cfg` (paso 1) solicita la configuración de CMC para el CMC activo y genera el archivo `miarchivo.cfg`. Si es necesario, se puede cambiar el nombre del archivo o guardarlo en una ubicación diferente.

Puede 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.

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 de la extensión `.cfg` (aunque en este apartado se haga referencia al mismo con esa denominación).



NOTA: Para obtener más información sobre `getconfig`, consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

RACADM analiza el archivo `.cfg` cuando este 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 estén siguiendo 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 esté 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`. Usted debe corregir todos los errores antes de poder realizar cualquier configuración.

Para verificar si hay 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 en 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.

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

Los índices se pueden crear y se pueden eliminar. Con el tiempo, el grupo se puede fragmentar con índices utilizados y no utilizados. Si hay un índice presente, este se modifica. Si no hay un índice presente, se utiliza el primer índice disponible. Este método ofrece flexibilidad al agregar anotaciones indexadas en las que no es necesario hacer correspondencias exactas del índice entre todos los CMC que se están administrando. 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.

- Utilice el subcomando `racresetcfg` para configurar ambos CMC con propiedades idénticas.

Utilice el subcomando `racresetcfg` para restablecer la configuración predeterminada original del CMC 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. Consulte el capítulo de propiedad de base de datos en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) para obtener una lista completa de objetos y grupos.

△ PRECAUCIÓN: Utilice el subcomando `racresetcfg` para restablecer la configuración predeterminada original de la base de datos y de la interfaz de red del CMC y para eliminar a todos los usuarios y las configuraciones de usuario. Aunque el usuario raíz está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Reglas de análisis

- Las líneas que comienzan con un carácter de almohadilla/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 leerán como caracteres `#`.

Algunos parámetros de módem pueden incluir caracteres `#` en sus cadenas. No se requiere un carácter de escape. Es recomendable generar un archivo `.cfg` a partir de un comando `racadm getconfig -f <nombre_de_archivo>.cfg` y luego ejecutar un comando `racadm config -f <nombre_de_archivo>.cfg` para otro CMC, sin agregar caracteres de escape.

Por ejemplo:

```
#
# Esto es un comentario
[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 producirán 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 la *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, el objeto y el valor de propiedad del objeto:

```
[cfgLanNetworking] -{nombre de grupo}
cfgNicIpAddress=143.154.133.121 {nombre de objeto}
{valor de objeto}
```

- Todos los parámetros están especificados 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 mantienen sin modificación. El carácter que se encuentre a la derecha del signo = (por ejemplo, un segundo signo = un #, [,], etc.) se tomará tal cual. Estos caracteres son caracteres de secuencia de comandos de conversación de módem válidos.

```
[cfgLanNetworking] -{nombre de grupo}
cfgNicIpAddress=143.154.133.121 {valor de objeto}
```

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

El usuario no puede especificar qué índice se va a utilizar. Si el índice ya existe, se utiliza o bien se crea la nueva anotación en el primer índice disponible de dicho grupo.

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




NOTA: Se puede crear un grupo indexado manualmente mediante el siguiente comando:

```
racadm config -g <nombre_de_grupo> -o <objeto anclado> -i <index 1-16> <nombre de anclaje único>
```

- La línea de un grupo indexado no se puede eliminar de un archivo `.cfg`. Si se elimina la línea con un editor de textos, RACADM se detendrá al analizar el archivo de configuración y producirá una alerta sobre el error. El usuario debe eliminar un objeto indexado manualmente con el siguiente comando:

```
racadm config -g <nombre_de_grupo> -o
<nombre_de_objeto> -i <índice 1-16> ""
```

 **NOTA:** Una cadena NULA (que se identifica por dos caracteres `"`) indica al CMC que elimine el índice del grupo especificado.

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

```
racadm getconfig -g <nombre_de_grupo> -i
<índice 1-16>
```

- Para grupos indexados, el ancla de objeto debe ser el primer objeto después del par `[]`. Los siguientes son ejemplos de los grupos indexados actuales:

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<NOMBRE_DE_USUARIO>
```

Si escribe `racadm getconfig -f <mi_ejemplo>.cfg`, el comando genera un archivo `.cfg` para la configuración actual del CMC. Este archivo de configuración se puede utilizar como ejemplo y como punto de partida para su archivo `.cfg` exclusivo.

Modificación de la dirección IP del CMC

Cuando modifique la dirección IP del CMC en el archivo de configuración, elimine todas las anotaciones de `<variable>=<valor>` innecesarias. Solo la etiqueta variable real del grupo con `[y]` permanece, incluyendo las dos anotaciones `<variable>=<valor>` correspondientes al cambio de la dirección IP.

Ejemplo:

```
N.º
```

```
# Grupo de objeto "cfgLanNetworking"
```

```
N.º
```

```
[cfgLanNetworking]
```

```
cfgNicIpAddress=10.35.10.110
```

```
cfgNicGateway=10.35.10.1
```

Este archivo se actualiza de la siguiente forma:

N.º

```
# Grupo de objeto "cfgLanNetworking"
```

N.º

```
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comentario, el resto de esta línea se ignora
cfgNicGateway=10.35.9.1
```

El comando `racadm config -f <myfile>.cfg` analiza el archivo e identifica todos los errores por número de línea. Un archivo correcto actualiza las anotaciones adecuadas. Además, usted puede usar el mismo comando `getconfig` que se usó en el ejemplo anterior para confirmar la actualización.

Utilice 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`.

Uso de RACADM para configurar propiedades en el iDRAC

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

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



NOTA: Para obtener más información sobre los valores y rangos predeterminados de la propiedad, consulte la Guía del usuario de Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise para servidores blade.

Si el firmware del 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
# cfgSsnMgtSSTimeout=N/A
# cfgSsnMgtTelnetMaxSessions=N/A
# cfgSsnMgtTelnetActiveSessions=N/A
# cfgSsnMgtTelnetTimeout=N/A
```

Solución de problemas

La Tabla 4-3 muestra problemas comunes relacionados con RACADM remoto.

Tabla 4-3. Uso de comandos serie/RACADM: Preguntas frecuentes

Pregunta	Respuesta
<p>Después de realizar un restablecimiento del CMC (mediante el subcomando <code>racreset</code> de RACADM), introducción un comando y se muestra el siguiente mensaje:</p> <pre>racadm <subcomando> Transport: ERROR: (RC=-1)</pre> <p>¿Qué significa este mensaje?</p>	<p>Debe esperar hasta que el CMC haya completado el restablecimiento antes de ejecutar otro comando.</p>
<p>Cuando uso los subcomandos de RACADM, aparecen errores que no comprendo.</p>	<p>Es posible que encuentre uno o más de los siguientes errores al utilizar RACADM:</p> <ul style="list-style-type: none"> • Mensajes de errores locales: problemas como sintaxis, errores tipográficos y nombres incorrectos. Ejemplo: <pre>ERROR: <mensaje></pre> <p>Utilice el subcomando <code>help</code> de RACADM para mostrar la sintaxis correcta y la información de uso.</p> • Mensajes de error relacionados con el CMC: problemas en los que el CMC no puede realizar una acción. También podría decir “el comando <code>racadm</code> falló”. <p>Escriba <code>racadm gettracelog</code> para obtener información sobre la depuración de errores.</p>

Tabla 4-3. Uso de comandos serie/RACADAM: Preguntas frecuentes (continuación)

Pregunta	Respuesta
Mientras estaba utilizando RACADM remoto, la petición cambió a ">" y no puedo hacer que regrese la petición "\$".	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 de espera. Para regresar a la petición "\$", presione <Ctrl>-d.
Intenté utilizar los siguientes comandos y recibí un error que indica "No se ha encontrado": \$ logout \$ quit	Los comandos logout y quit no se admiten en la interfaz de la CLI del CMC.

Uso de la interfaz web del CMC

El iDRAC6 ofrece una interfaz web que permite configurar las propiedades y los usuarios del CMC, realizar tareas de administración remota y solucionar problemas de un sistema (administrado) remoto. Para la administración diaria del chasis, utilice la interfaz web del CMC. En este capítulo se proporciona información acerca de cómo realizar tareas de administración del chasis por medio de la interfaz web del CMC.

También puede realizar todas las tareas de configuración de la interfaz web con los comandos de RACADM local o las consolas de línea de comandos (consola serie, Telnet o SSH). Para obtener más información acerca del uso RACADM local, ver “Uso de la interfaz de línea de comandos de RACADM” en la página 79. Para obtener información acerca de cómo utilizar las consolas de línea de comandos, consulte la sección “Configuración del CMC para el uso de consolas de línea de comandos” en la página 65.



NOTA: Si utiliza 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.

Acceso a la interfaz web del CMC

Para acceder a la interfaz web del CMC mediante IPv4:

- 1 Abra una ventana de un explorador web compatible.

Para obtener información actualizada sobre los exploradores web admitidos, consulte la *Dell Systems Software Support Matrix* que se encuentra en support.dell.com/manuals.

- 2 Escriba el siguiente URL en el campo Dirección y luego presione <Intro>:

`https://<dirección IP de CMC>`

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

`https://<dirección IP de CMC>:<número de puerto>`

donde <dirección IP de CMC> es la dirección IP del CMC y <número de puerto> corresponde al número de puerto HTTPS.


Aparece la página de Inicio de sesión de CMC.

Para acceder a la interfaz web del CMC mediante IPv6:

- 1 Abra una ventana de un explorador web compatible.

Para obtener información actualizada sobre los exploradores web admitidos, consulte la *Dell Systems Software Support Matrix* que se encuentra en support.dell.com/manuals.

- 2 Escriba el siguiente URL en el campo **Dirección** y luego presione <Intro>:
`https://[<dirección IP de CMC >]`

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


La especificación del número de puerto HTTPS en la URL es opcional si todavía está utilizando el valor predeterminado (443). De lo contrario, debe especificar el número de puerto. La sintaxis para la URL IPv6 del CMC con especificación del número de puerto es:


`https://[<dirección IP de CMC >]:<port number>`

donde <dirección IP de CMC > es la dirección IP del CMC y <número de puerto> corresponde al número de puerto HTTPS.


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

Inicio de sesión

 **NOTA:** Para iniciar sesión en el CMC, debe tener una cuenta del CMC con privilegios para **Iniciar sesión en el CMC**.



 **NOTA:** El nombre de usuario predeterminado de la CMC es *raíz*, y la contraseña es *calvin*. La cuenta raíz es la cuenta administrativa predeterminada que se incluye con el CMC. Para mayor seguridad, se recomienda cambiar la contraseña predeterminada de la cuenta raíz durante la configuración inicial.

 **NOTA:** El CMC no admite caracteres ASCII extendidos, como por ejemplo ß, â, é, ü u otros caracteres utilizados principalmente en idiomas distintos al inglés.

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


Puede iniciar sesión como usuario de CMC o como usuario de Active Directory.

Para iniciar sesión:

- 1 En el campo **Nombre de usuario**, escriba su nombre de usuario:
 - Nombre de usuario de la 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 en LDAP: *<nombre de usuario>*
-  **NOTA:** Este campo distingue entre mayúsculas y minúsculas.
- 2 En el campo **Contraseña**, escriba la contraseña de usuario de la CMC o de Active Directory.
-  **NOTA:** Este campo distingue entre mayúsculas y minúsculas.
- 3 De forma opcional, puede seleccionar un límite de tiempo de espera para la sesión. El tiempo de espera es el plazo en el que puede permanecer conectado sin actividad antes de que el sistema cierre la sesión automáticamente. El valor predeterminado es el tiempo de espera en inactividad del servicio web. Para obtener más información, consulte Configuración de servicios.
- 4 Haga clic en **Aceptar** o presione **<Intro>**.

Cierre de sesión

Cuando inicia sesión en la interfaz web, usted puede desconectarse en cualquier momento si hace clic en **Desconectar** en la esquina superior derecha de cualquier página.

 **NOTA:** Tenga cuidado de aplicar (guardar) todos los valores o la información que introduzca en una página. Si se desconecta o se desplaza a otra página sin aplicar los cambios, estos se perderán.


Configuración de los valores básicos del CMC

En las secciones siguientes se proporciona información sobre cómo configurar los valores básicos 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 “Sistema de estante Dell”). Por ejemplo, una consulta SNMP sobre el nombre del chasis devuelve el nombre que haya configurado.

Para establecer el nombre y la ubicación del chasis:

- 1 Inicie sesión en la interfaz web del CMC.
Aparecerá la página **Condición del chasis**.
- 2 Haga clic en la ficha **Configuración**.
Aparecerá la página **Configuración general del chasis**.
- 3 Escriba las propiedades de ubicación en los campos **Centro de datos**, **Pasillo**, **Bastidor** y **Ranura del bastidor**.
 **NOTA:** El campo Ubicación del chasis es opcional. Se recomienda utilizar los campos **Centro de datos**, **Pasillo**, **Bastidor** y **Ranura del bastidor** para indicar la ubicación física del chasis.
- 4 Escriba el nuevo nombre en el campo **Nombre del chasis** y luego haga clic en **Aplicar**.

Establecimiento de la fecha y la hora en el CMC

Puede definir la fecha y la hora manualmente, o puede sincronizar la fecha y la hora con un servidor de protocolo de hora de red (NTP). Para establecer la fecha y hora en el CMC:

- 1 Inicie sesión en la interfaz web del CMC.
Aparecerá la página **Condición del chasis**.
- 2 Haga clic en la ficha **Configuración**.
Aparecerá la página **Configuración general del chasis**.
- 3 Haga clic en la subficha **Fecha/Hora**.
Aparecerá la página **Fecha/Hora**.
- 4 Para sincronizar la fecha y la hora con un protocolo de hora de red (NTP), seleccione **Activar NTP** y especifique hasta tres servidores NTP.
- 5 Para establecer la fecha y la hora manualmente, deselectione **Activar NTP** y edite los campos **Fecha** y **Hora**, seleccione la **Zona horaria** del menú desplegable y haga clic en **Aplicar**.

Para establecer la fecha y la hora mediante la interfaz de línea de comandos, consulte las secciones del comando `config` y del grupo de propiedad de base de datos `cfgRemoteHosts` en la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC).

Activación de soportes flash extraíbles

Puede reparar o activar el soporte flash extraíble opcional para utilizar como un almacenamiento ampliado y no volátil. Algunas funciones del CMC dependen de almacenamiento ampliado y no volátil para funcionar.

Para reparar o activar el soporte flash extraíble:

- 1 Inicie sesión en la interfaz web del CMC.
Aparecerá la página **Condición del chasis**.
- 2 Haga clic en **Controlador del chasis** en la lista en forma de árbol.
Aparecerá la página **Estado de la controladora del chasis**.
- 3 Haga clic en la ficha **Medios flash**.
Aparecerá la página **Medios flash extraíbles**.
- 4 Para empezar a utilizar el soporte, seleccione **Utilizar medio para almacenar datos del chasis** en la lista desplegable.
- 5 Si el soporte en un CMC parece que tiene un problema, active ese CMC y seleccione **Preparar o reparar el medio de la controladora activa** en la lista desplegable.

Si hay dos CMC en el chasis, ambos deben contener un soporte flash. Las funciones del CMC que dependen del soporte flash (excepto Flexaddress), no funcionan correctamente hasta que se ha instalado y activado en esta página un soporte autorizado por Dell.

Página de condición del chasis

Al iniciar sesión en CMC, se abre la página **Condición del chasis** (**Descripción general del chasis**→**Propiedades**→**Condición**). En esta página se muestran la información y las acciones que se necesitan con más frecuencia. Si su chasis está configurado como Líder de grupo, cuando inicie sesión se abrirá la página **Condición del grupo**. Para obtener más información, consulte “Cómo utilizar el grupo de chasis” en la página 120.

La página **Condición del chasis** muestra una vista gráfica en vivo del chasis y sus componentes, además de información detallada sobre estos componentes. De acuerdo con el componente seleccionado, se encuentran disponibles diferentes acciones o vínculos a otras páginas. Además se muestran los últimos sucesos en el registro de hardware de CMC.

Toda la información de la página **Condición del chasis** se actualiza dinámicamente. La página contiene dos secciones principales: **Resumen de componentes del chasis** en la parte superior y después la lista **Sucesos recientes del registro de hardware de CMC**.

La sección **Resumen de componentes del chasis** (que también lleva el título “Condición del chasis” cuando ofrece información general del chasis) muestra representaciones gráficas y la información relacionada. Al hacer clic en el icono **Cerrar**, es posible ocultar por completo esta sección.

La mitad izquierda de la sección **Resumen de componentes del chasis** muestra gráficos y vínculos de acceso rápido del chasis. La mitad derecha de la sección muestra información, vínculos y acciones relacionadas con el componente seleccionado. Haga clic en la representación gráfica de un componente para seleccionarlo. El gráfico adquiere un color azul después de seleccionarlo.

La lista **Sucesos recientes del registro de hardware de CMC** muestra los 10 sucesos más recientes del registro. El contenido de esta sección se actualiza dinámicamente y se presenta con el último suceso en el primer lugar de la lista. Para obtener más información sobre las anotaciones del registro de hardware de CMC, ver “Cómo ver los registros de sucesos” en la página 455.

Cómo utilizar el grupo de chasis

CMC le permite controlar varios chasis desde un chasis líder o principal. Cuando se activa un Grupo de chasis, el CMC del chasis principal genera un mensaje gráfico sobre el estado del chasis principal y de los demás chasis del grupo.

Características del grupo de chasis

El grupo de chasis tiene las siguientes características:

- En la página de la interfaz gráfica de usuario del grupo de chasis se muestran imágenes de la parte anterior 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 secundarios se marcan en rojo o amarillo y con una **X** o una **!** 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 el botón **Detalles**.

- Los vínculos de inicio rápido están disponibles para abrir chasis de miembros o servidores de páginas web.
- Hay un inventario de entradas/salidas y un blade disponibles para un grupo.
- Existe una opción seleccionable para sincronizar las propiedades del miembro nuevo con las propiedades del principal cuando se añade un miembro nuevo al grupo.

Cómo configurar un grupo de chasis

Un grupo de chasis puede contener hasta ocho miembros. Además, en cada grupo puede haber un líder. Un chasis que pertenece a un grupo, ya sea como miembro o como líder, no se puede unir a otro grupo. Puede eliminar el chasis de un grupo y añadirlo más tarde a un grupo diferente.

Para configurar el grupo de chasis mediante la interfaz gráfica de usuario:

- 1 Inicie sesión con privilegios de administrador de chasis en el chasis que se va a configurar como principal.
- 2 Haga clic en **Configurar**→ **Administración de grupo**.
Aparecerá la página **Grupo de chasis**.
- 3 En la página **Grupo de chasis**, en **Función**, seleccione **Líder**.
Se mostrará un campo para añadir el nombre del grupo.
- 4 Introduzca el **Nombre del grupo** en el campo correspondiente 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 de la interfaz del grupo de chasis. El árbol del sistema indica el grupo por nombre de grupo y el chasis principal y el chasis sin nombres de miembros aparecen en el árbol del sistema.

Después de configurar el grupo de chasis, puede añadir miembros al grupo:

- 1 Inicie sesión en el chasis principal con privilegios de administrador de chasis.
- 2 Seleccione el chasis principal en el árbol.
- 3 Haga clic en **Configurar**→ **Administración de grupo**.
- 4 En **Administración de grupo**, introduzca el nombre DNS o la dirección IP del miembro en el campo **Nombre del host/Dirección IP**.
- 5 Introduzca un nombre de usuario con privilegios de administrador de chasis en el chasis miembro, en el campo **Nombre de usuario**.

- 6 Introduzca la contraseña correspondiente en el campo **Contraseña**.
- 7 También tiene la opción de seleccionar **Sincronizar el miembro nuevo con las propiedades del principal** para enviar las propiedades del chasis principal al nuevo. Para obtener más información, consulte la subsección “Sincronización de un miembro nuevo con las propiedades del chasis principal” en la página 124.
- 8 Haga clic en el botón **Aplicar**.
- 9 Repita los pasos del paso 4 al paso 8 para añadir miembros, hasta un máximo de ocho.
Los nombres de chasis de los miembros nuevos aparecen en el cuadro de diálogo **Miembros**.

Al seleccionar un grupo del árbol se muestra el estado del miembro nuevo. Al hacer clic en la imagen del chasis o el botón de detalles, aparecen los detalles.



NOTA: Las credenciales de 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 pedir una vez que se ha establecido la relación de confianza.

Cómo eliminar un miembro del chasis principal.

Puede eliminar un miembro del grupo desde el chasis principal. Para eliminar un miembro deberá realizar lo siguiente:

- 1 Inicie sesión en el chasis principal con privilegios de administrador de chasis.
- 2 Seleccione el chasis principal en el árbol.
- 3 Haga clic en **Configurar** → **Administración de grupo**.
- 4 En la lista **Quitar miembros**, seleccione el nombre o los nombres de los miembros que se van a eliminar y haga clic en **Aplicar**.

El chasis principal establecerá una conexión con el miembro o miembros, si se selecciona más de uno, que se han eliminado del grupo. El nombre de miembro desaparece del cuadro de diálogo. Si debido a un problema en la red no se produce un contacto entre el miembro y el líder es posible que el chasis miembro no reciba el mensaje. Si esto se produce, desactive el miembro del chasis miembro para poder quitarlo totalmente. Para obtener más información, consulte la subsección “Cómo desactivar un miembro del chasis miembro” en la página 123.

Cómo desmontar un grupo de chasis

Para extraer totalmente un grupo del chasis principal:

- 1 Inicie sesión en el chasis principal con privilegios de administrador de chasis.
- 2 Seleccione el chasis principal en el árbol.
- 3 Haga clic en **Configurar**→ **Administración de grupo**.
- 4 En la página **Grupo de chasis**, en **Función**, seleccione **Ninguno** y, a continuación, haga clic en **Aplicar**.

El chasis principal establecerá una conexión con todos los miembros que se han quitado del grupo. Finalmente, el chasis principal finalizará su función. Ahora se le puede nombrar como miembro o líder de otro grupo.

Si debido a un problema en la red no se produce un contacto entre el miembro y el líder es posible que el chasis miembro no reciba el mensaje. Si esto se produce, desactive el miembro del chasis miembro para poder quitarlo totalmente. Para obtener más información, consulte la subsección “Cómo desactivar un miembro del chasis miembro” en la página 123.

Cómo desactivar 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 de chasis.
- 2 Haga clic en **Configurar**→ **Administración de grupo**.
- 3 Seleccione **Ninguno** y, a continuación, haga clic en **Aplicar**.

Cómo iniciar la página web del servidor o de un chasis miembro

Los vínculos a la página web de un chasis miembro, la consola remota de un servidor o la página web del servidor iDRAC dentro del grupo están disponibles a través de la página del grupo del chasis principal. Puede utilizar el nombre de usuario y la contraseña con los que 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 será 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 es un CMC miembro, seleccione **Iniciar CMC** debajo del chasis adecuado.

Si el destino es un servidor en un chasis haga 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 **Vínculos rápidos** seleccione el dispositivo de destino.

Aparecerá una nueva ventana con la página de destino o la pantalla de inicio de sesión.

Sincronización de un miembro nuevo con las propiedades del chasis principal

Las propiedades del chasis principal se pueden aplicar a un chasis miembro que se acaba de añadir a un grupo. Para sincronizar un nuevo miembro con las propiedades del principal:

- 1 Inicie sesión en el chasis principal con privilegios de administrador de chasis.
- 2 Seleccione el chasis principal en el árbol.
- 3 Haga clic en **Configurar** → **Administración de grupo**.
- 4 Al añadir un miembro nuevo al grupo, en la página **Grupo de chasis**, seleccione **Sincronizar el miembro nuevo con las propiedades del principal**.
- 5 Haga clic en **Aplicar**.

El miembro adquirirá las propiedades del principal.

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

Tabla 5-1. Propiedades del servicio de configuración

Propiedad	Navegación
Configuración de SNMP	Haga clic en Descripción general del chasis → Red → Servicios → SNMP para conocer los detalles.
Registro remoto del chasis	Haga clic en Descripción general del chasis → Red → Servicios → Syslog remoto para conocer los detalles.
Autenticación de usuario con LDAP y Active Directory	Haga clic en Descripción general del chasis → Autenticación de usuarios → Servicios de directorios para conocer los detalles.
Alertas del chasis	Haga clic en Descripción general del chasis → Alertas para conocer los detalles.

Inventario de blade para el grupo de MCM

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

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

Cómo guardar el informe de inventario de blade

Para guardar el informe de inventario de blade:

- 1** Inicie sesión en la interfaz web del CMC y seleccione **Grupo** en el árbol del sistema.

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

- 2** Haga clic en el botón **Guardar el informe de inventario**.

Se mostrará el cuadro de diálogo **Descarga de archivo**, donde se le solicitará que abra o guarde el archivo.

- Haga clic en **Guardar** y especifique la ruta de acceso y el nombre del archivo para el informe de inventario de blade.



NOTA: El chasis principal y los chasis miembro del grupo, así como las blade del chasis asociado, deben estar **encendidos** para que el informe de inventario de blade sea lo más preciso posible.

Datos exportados

El informe de inventario de blade contiene los datos más recientes que devolvió cada miembro del grupo de chasis durante el sondeo normal del chasis principal del grupo (una vez cada 30 segundos).

Para obtener el informe de inventario de blade más preciso posible:

- El chasis principal y todos los chasis miembro del grupo deben estar **encendidos**
- Todas las blade del chasis asociado deben estar encendidas

Es posible que el informe de inventario no incluya los datos de inventario del chasis asociado y las blade si un subconjunto de chasis miembro del grupo está:

- En estado de alimentación del chasis apagado
- Apagado

En la Tabla 5-2 se indican los campos de datos específicos y los requisitos específicos para los campos que se incluirán en el informe de cada blade:

Tabla 5-2. Descripciones de campos del 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	SLOT-01
Nombre del host	servidor de web corporativo

NOTA: Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.

Tabla 5-2. Descripciones de campos del inventario de blade

Campo de datos	Ejemplo
Operating System (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 GB NOTA: Requiere CMC 4.0 (o superior) en el miembro; de lo contrario, se mostrará en blanco.
N.º de CPU	2 NOTA: Requiere CMC 4.0 (o superior) en el miembro; de lo contrario, se mostrará en blanco.
Información de la CPU	CPU Intel (R) Xeon (R) E5502 a 1,87 GHz 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 puede importar en varias herramientas tales como, por ejemplo, Microsoft Excel. El archivo **.CSV** del informe de inventario se puede importar en la plantilla seleccionando **Datos**→ **Desde el texto** en MS Excel. Una vez que el informe de inventario se haya importado en MS Excel, si se muestra un mensaje para solicitarle más información, seleccione Delimitado por comas para importar el archivo en MS Excel.

Resumen de componentes del chasis

En las secciones siguientes se proporciona información sobre el resumen de componentes del chasis.

Gráficos del chasis

Las vistas anterior 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 por medio del color azul y se controla al hacer clic sobre la imagen del componente deseado. 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 por medio de un fondo de color gris oscuro. El icono del componente indica visualmente su estado. En la Tabla 5-1, el icono de servidor se utiliza a modo de ejemplo. Otros componentes muestran iconos que los representan visualmente. 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 aparece información adicional sobre ese componente.

Tabla 5-3. Estados del icono del servidor






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

Tabla 5-3. Estados del icono del servidor (continuación)

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

En la Tabla 5-4 se muestran los vínculos de acceso rápido al chasis.

Tabla 5-4. Vínculos de acceso rápido del chasis

Campo	Descripción
Configurar usuarios	Vaya a Descripción general del chasis → Autenticación de usuario → Usuarios locales
Configuración de la red	Vaya a Descripción general del chasis → Red → Red
Configuración de la alimentación	Vaya a Descripción general del chasis → Alimentación → Configuración
Actualización del firmware	Vaya a Descripción general del chasis → Actualizar → Actualización del firmware

Condición del chasis

Cuando se abre la primera página, el lado derecho muestra alertas e información sobre el nivel del chasis. Se presentan todas las alertas activas críticas y no críticas.

Al hacer clic en un componente, la información de nivel del chasis es reemplazada por información sobre el componente seleccionado. Para regresar a la información sobre el nivel del chasis, haga clic en **Volver a la condición del chasis** en la esquina superior derecha.

Tabla 5-5. Información de la página del chasis

Campo	Descripción
Modelo	Muestra el modelo del panel LCD del chasis.
Firmware	Muestra la versión de firmware del CMC activo.
Etiqueta de servicio	Muestra la etiqueta de servicio del chasis. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para fines de asistencia y mantenimiento.
Asset Tag (Etiqueta de propiedad)	Muestra la etiqueta de propiedad del chasis.
Alimentación de entrada	Indica la cantidad de alimentación eléctrica que el chasis consume en ese momento.
Límite de alimentación	La alimentación de entrada máxima que puede consumirse, de acuerdo con el valor asignado por el usuario. Cuando el chasis alcanza este límite, los servidores comienzan a regularse para evitar un mayor aumento de la alimentación de entrada requerida.
Política de alimentación	Preferencia asignada por el usuario para coordinar varias unidades de suministro de energía.
Condición	Muestra la condición general del subsistema de alimentación del chasis.

Información del componente seleccionado

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

- Las secciones de condición, rendimiento y propiedades.

Los sucesos activos críticos y no críticos de los registros de hardware, de existir, se muestran en esta sección. Aquí también se muestran los datos de rendimiento que varían con el transcurso del tiempo.

- **Properties**
En esta sección se muestran las propiedades de los componentes que no varían con el tiempo o cambian solo excepcionalmente.
- **Vínculos de acceso rápido**
La sección de vínculos de acceso rápido ofrece una forma sencilla para dirigirse a las páginas y las acciones que se acceden con más frecuencia. En esta sección solo se muestran los vínculos correspondientes al componente seleccionado.

Tabla 5-6. Información de condición y rendimiento: Servidores

Elemento	Descripción
Estado de la alimentación	Estado de encendido o apagado del servidor. Ver Tabla 5-25 para obtener información detallada sobre los diversos tipos de estados de la alimentación.
Condición	Muestra el texto equivalente al icono de condición.
Power Consumption	Indica la cantidad de alimentación eléctrica que el servidor consume en este momento.
Energía asignada	Es la cantidad de energía presupuestada para el servidor.
Temperatura	La lectura obtenida por el sensor de temperatura del servidor.

Tabla 5-7. Propiedades de servidor

Elemento	Descripción
Nombre	Nombre de ranura asignado por el usuario.
Modelo	Modelo de servidor, por ejemplo “PowerEdge M600” o “PowerEdge M605”.
Etiqueta de servicio	La etiqueta de servicio del servidor. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para fines de asistencia y mantenimiento. Si el servidor está ausente, este campo está vacío.
Sistema operativo	El sistema operativo del servidor.
Nombre del host	El nombre del servidor según lo establece el sistema operativo.

Tabla 5-7. Propiedades de servidor (continuación)

Elemento	Descripción
iDRAC	La versión del firmware del iDRAC en el servidor.
BIOS	La versión del BIOS del servidor.
CPLD	Número de versión del dispositivo lógico programable complejo (CPLD) del servidor.
Información de CPU	Muestra el número, y el tipo, de CPU instaladas en el servidor.
Memoria total del sistema	Muestra la memoria total del sistema (en GB) instalada en el servidor.

Tabla 5-8. Vínculos de acceso rápido: Servidores

Elemento	Descripción
Estado del servidor	Vaya a Descripción general de servidores → <servidor seleccionado>→ Propiedades → Estado .
Iniciar la consola remota	Abre una sesión de teclado, video y mouse (KVM) en el servidor si este admite esta operación.
Iniciar la interfaz gráfica de usuario del iDRAC	Abre una consola de administración del iDRAC para el servidor.
Encender el servidor	Aplica energía a un servidor que está en estado “Apagado”.
Apagar el servidor	Quita la energía de un servidor que está en estado “Encendido”.
Recurso compartido de archivos remotos	Vaya a Descripción general de servidores → Configuración → Recurso compartido de archivos remotos
Implementar red de iDRAC	Vaya a Descripción general de servidores → Configuración → iDRAC (Implementar iDRAC) .
Controlador del ciclo de vida	Vaya a Descripción general de servidores → Actualizar → Actualización del firmware .

Tabla 5-9. Condición y rendimiento del módulo de E/S

Elemento	Descripción
Estado de la alimentación	Muestra el estado de alimentación del módulo de E/S: Encendido, Apagado o Desconocido (ausente).
Función	Muestra la membresía del módulo de E/S respecto de una pila cuando los módulos se vinculan entre sí. La membresía indica que el módulo es parte de un conjunto de pilas. La calificación “maestro” indica que el módulo es un punto de acceso primario.

Tabla 5-10. Propiedades del módulo de E/S

Elemento	Descripción
Modelo	Muestra el nombre de producto del módulo de E/S.
Etiqueta de servicio	Muestra la etiqueta de servicio del módulo de E/S. La etiqueta de servicio es un identificador exclusivo que Dell asigna para fines de asistencia técnica y mantenimiento.

Tabla 5-11. Vínculos de acceso rápido: módulos de E/S

Elemento	Descripción
Estado del módulo de E/S	Vaya a Módulos de E/S → <Módulos de E/S seleccionados> → Propiedades → Estado .
Iniciar interfaz gráfica de usuario del módulo de E/S	Si se muestra el vínculo <i>Iniciar interfaz gráfica de usuario del módulo de E/S</i> para un módulo de E/S particular, al hacer clic en el vínculo se iniciará la consola de administración de módulos de E/S correspondiente a ese módulo en una nueva ventana o ficha del navegador.

Tabla 5-12. Condición y rendimiento del CMC activo

Elemento	Descripción
Modo de redundancia	Muestra la capacidad de protección contra fallas del CMC en espera. Si el firmware del CMC no coincide o el CMC no está correctamente conectado a la red de administración, la redundancia aparece como no disponible.
Dirección MAC	Muestra la dirección MAC de la tarjeta de interfaz de red (NIC) del CMC. La dirección MAC es un identificador único del CMC en toda la red.
IPv4	Muestra la dirección IPv4 actual de la interfaz de red del CMC.
IPv6	Muestra la primera dirección IPv6 de la interfaz de red del CMC.

Tabla 5-13. Propiedades de CMC

Elemento	Descripción
Firmware	Muestra la versión de firmware del CMC activo.
Firmware en espera	Muestra la versión del firmware que está instalado en el CMC en espera. Si no hay un segundo CMC instalado, en este campo se muestra el valor NA.
Última actualización	Muestra la fecha en la que el firmware se actualizó por última vez. Si no hubo actualizaciones, en este campo se muestra el valor NA.
Hardware	Muestra la versión de hardware del CMC activo.

Tabla 5-14. Vínculos de acceso rápido: CMC

Elemento	Descripción
Estado del CMC	Vaya a Controlador del chasis → Propiedades → Estado .
Funciones de red	Vaya a Descripción general del chasis → Red → Red .
Actualización del firmware	Vaya a Descripción general del chasis → Actualizar → Actualización del firmware .

Tabla 5-15. Condición y rendimiento de iKVM

Elemento	Descripción
Consola OSCAR	Muestra si el conector VGA del panel posterior está activado (Sí o No) para el acceso a CMC.

Tabla 5-16. Propiedades de iKVM

Elemento	Descripción
Nombre	Muestra el nombre del iKVM.
Número de parte	Muestra el número de parte del iKVM. El número de parte es un identificador único que el proveedor proporciona. Las convenciones de notación de los números de parte varían de un proveedor a otro.
Firmware	Muestra la versión del firmware del iKVM.
Hardware	Muestra la versión de hardware del iKVM.

Tabla 5-17. Vínculos de acceso rápido: iKVM

Elemento	Descripción
Estado del iKVM	Vaya a iKVM → Propiedades → Estado .
Actualización del firmware	Vaya a Descripción general del chasis → Actualización → Actualización del firmware .

Tabla 5-18. Condición y rendimiento del ventilador

Elemento	Descripción
Velocidad	Muestra la velocidad del ventilador en revoluciones por minuto (RPM).

Tabla 5-19. Propiedades del ventilador

Elemento	Descripción
Umbral crítico inferior	Velocidad por debajo de la cual se considera que hay una falla del ventilador.
Umbral crítico superior	Velocidad por arriba de la cual se considera que hay una falla del ventilador.

Tabla 5-20. Vínculos de acceso rápido: ventilador

Elemento	Descripción
Estado del ventilador	Vaya a Ventiladores→ Propiedades→ Estado.

Tabla 5-21. Condición y rendimiento de las unidades de suministro de energía

Elemento	Descripción
Estado de la alimentación	Muestra el estado de la alimentación de los suministros de energía: Inicializando, En línea, En espera, En diagnóstico, Fallido, Actualización, Fuera de línea o Desconocido.

Tabla 5-22. Propiedades de las unidades de suministro de energía

Elemento	Descripción
Capacidad	Muestra la capacidad del suministro de energía (en vatios).

Tabla 5-23. Vínculos de acceso rápido: unidades de suministro de energía

Elemento	Descripción
Estado del suministro de energía	Vaya a Suministros de energía→ Propiedades→ Estado.
Power Consumption	Vaya a Descripción general del chasis→ Alimentación→ Consumo de alimentación.
Presupuesto del sistema	Vaya a Descripción general del chasis→ Alimentación→ Estado del presupuesto.

Tabla 5-24. Condición y rendimiento de LCD

Elemento	Descripción
Condición de LCD	Muestra la presencia y la condición de la pantalla LCD.
Condición del chasis	Muestra la descripción en formato de texto de la condición del chasis.

No hay vínculos de acceso rápido para la pantalla LCD.

Supervisión del estado de la condición del sistema

Cómo ver los resúmenes del chasis y los componentes

El CMC muestra una representación gráfica del chasis en la página **Condición del chasis** que ofrece una descripción visual del estado de los componentes instalados. La página **Condición del chasis** se actualiza en forma dinámica y los cuadros de texto y los niveles de los gráficos secundarios de los componentes cambian automáticamente para reflejar el estado actual.

Ilustración 5-1. Ejemplo de gráficos de chasis en la interfaz web



La página **Condición del chasis** ofrece el estado de la condición general del chasis, los CMC activos y en espera, los módulos de servidor, los módulos de E/S, los ventiladores, iKVM, los suministros de energía (unidades de suministro de energía) y la pantalla LCD. Haga clic en un componente para obtener información detallada sobre él. Para obtener instrucciones acerca de cómo ver el chasis y los resúmenes de los componentes, ver “Cómo ver los resúmenes del chasis” en la página 450.

Cómo ver el estado del presupuesto de alimentación

La página **Estado de presupuesto de alimentación** muestra el estado del presupuesto de alimentación del chasis, los servidores y las unidades de suministro de energía (PSU) del chasis.

Para obtener instrucciones acerca de cómo ver el estado del presupuesto de alimentación, ver “Cómo ver el estado del consumo de alimentación” en la página 359. Para obtener más información acerca de la administración de la alimentación en el CMC, ver “Administración de la alimentación” en la página 333.

Cómo ver el nombre de modelo del servidor y etiqueta de servicio

El nombre del modelo y la etiqueta de servicio de cada servidor se pueden obtener de manera instantánea mediante los pasos siguientes:

- Cómo expandir la rama Servidores en el árbol del sistema. Todos los servidores (1 a 16) aparecen en la lista expandida de servidores. Una ranura sin un servidor tendrá su nombre desactivado.
- Al pasar el cursor sobre el nombre o el número de ranura de un servidor, aparece información sobre el nombre de modelo del servidor y la etiqueta de servicio (si la información está disponible).

Cómo ver el estado de la condición de todos los servidores

El estado de todos los servidores puede verse en la sección **Gráficos del chasis** de la página **Condición del chasis** o la página **Estado de servidores**.

Gráficos del chasis proporciona una descripción gráfica de todos los servidores instalados en el chasis.

Para ver la condición de todos los servidores a través de Gráficos del chasis:

- 1 Inicie sesión en la interfaz web del CMC.

Aparecerá la página **Condición del chasis**. La sección izquierda de **Gráficos del chasis** muestra la vista frontal del chasis y contiene la condición de todos los servidores. El estado de la condición del servidor se indica mediante la superposición de niveles del gráfico secundario del servidor:

- Sin superposición: el servidor está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
- Señal de precaución de color ámbar: indica que solo se emitieron alertas de aviso y deben tomarse medidas correctivas.

- X de color rojo: indica que existe al menos una condición de falla. Esto significa que el CMC aún se puede comunicar con el componente y que el estado de la condición sobre la que se informa es crítico.
- Color gris: indica que el componente está presente y no está encendido. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.

La página **Estado de los servidores** proporciona descripciones generales de los servidores en el chasis. Para ver el estado de la condición de todos los servidores por medio de la página Estado de servidores:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de servidores** en el árbol del sistema.
Aparecerá la página **Estado de los servidores**.

Tabla 5-25. Información del estado de todos los servidores

Elemento	Descripción
Ranura	Muestra la ubicación del servidor. El número de ranura es un número progresivo que identifica al módulo del servidor por su ubicación dentro del chasis.
Nombre	Muestra el nombre del servidor, que de manera predeterminada se identifica mediante su nombre de ranura (RANURA-01 a RANURA-16). NOTA: El nombre de servidor predeterminado puede modificarse. Para obtener instrucciones, ver “Edición de los nombres de ranuras” en la página 142.
Modelo	Muestra el nombre del modelo del servidor. Si este campo está en blanco, el servidor no está presente. Si este campo muestra Extensión de n.º (donde el n.º es de 1 a 8), ese número corresponde a la ranura principal de un servidor con múltiples ranuras.

Tabla 5-25. Información del estado de todos los servidores *(continuación)*





Elemento	Descripción
Condición	 <p>En buen estado</p> <p>Muestra que el servidor está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar el estado de la condición del servidor.</p>
	 <p>Información</p> <p>Muestra información acerca del servidor cuando no se ha producido ningún cambio en el estado de la condición (En buen estado, Advertencia, Crítico).</p>
	 <p>Aviso</p> <p>Muestra que solo se emitieron alertas de aviso y <i>que deben tomarse medidas correctivas</i>. Si no se toman medidas correctivas, existe la posibilidad de que surjan fallas críticas que pueden afectar la integridad del dispositivo.</p>
	 <p>Crítico</p> <p>Muestra que se ha enviado al menos una alerta de falla. El estado crítico representa una falla del sistema en el servidor y <i>se debe tomar acción correctiva inmediatamente</i>.</p>
	<p>Sin valor</p> <p>Cuando el servidor no está presente en la ranura, no se proporciona información de su condición.</p>
<p>Iniciar la consola remota</p> <p>Haga clic para iniciar una sesión de teclado, video y mouse (KVM) en el servidor en una nueva ventana o ficha del explorador. Este icono solamente se visualiza para un servidor cuando se cumplen todas las condiciones siguientes:</p> <ul style="list-style-type: none"> • Servidores que admiten iDRAC6 e iDRAC7. • El chasis está encendido. • La interfaz de LAN en el servidor está activada. • La versión del iDRAC es 2.20 o superior. <p>Esta función solo se ejecuta correctamente si se cumplen las siguientes condiciones:</p> <ul style="list-style-type: none"> • El sistema host está instalado con JRE (Java Runtime Environment) 6 Update 16 o superior. • El explorador o el sistema host admiten el uso de ventanas emergentes (el bloqueo de ventanas emergentes está desactivado) 	

Tabla 5-25. Información del estado de todos los servidores (continuación)

Elemento	Descripción
Iniciar la interfaz gráfica de usuario del iDRAC	<p>Haga clic en el botón para iniciar la consola de administración del iDRAC para un servidor en una nueva ventana o ficha del explorador. Este icono solamente se visualiza para un servidor cuando se cumplen todas las condiciones siguientes:</p> <ul style="list-style-type: none">• El servidor está presente.• El chasis está encendido.• La interfaz de LAN en el servidor está activada. <p>Esta función solo se ejecuta correctamente si se cumplen las siguientes condiciones:</p> <ul style="list-style-type: none">• El explorador o el sistema host admiten el uso de ventanas emergentes (el bloqueo de ventanas emergentes está desactivado) <p>NOTA: Si un servidor se quita del chasis, se cambia la dirección IP del iDRAC o la conexión de red del iDRAC no funciona, entonces al hacer clic en el icono Iniciar interfaz gráfica de usuario del iDRAC puede aparecer una página de error en la interfaz LAN del iDRAC.</p>
Estado de la alimentación	<p>Muestra el estado de la alimentación del servidor:</p> <ul style="list-style-type: none">• N/A: el CMC no ha determinado aún el estado de la alimentación del servidor.• Apagado: el servidor o el chasis están apagados.• Encendido: tanto el chasis como el servidor están encendidos.• Encendiendo: estado temporal entre Apagado y Encendido. Cuando la acción finalice satisfactoriamente, el Estado de la alimentación estará Encendido.• Apagando: estado temporal entre Encendido y Apagado. Cuando la acción finalice satisfactoriamente, el Estado de la alimentación estará Apagado.
Etiqueta de servicio	<p>Muestra la etiqueta de servicio del servidor. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento. Si el servidor está ausente, este campo está vacío.</p>

Para obtener información acerca de cómo iniciar la consola de administración del iDRAC y políticas de inicio de sesión único, ver “Cómo iniciar el iDRAC mediante el inicio de sesión único” en la página 239.

Edición de los nombres de ranuras

La página **Nombres de ranuras** le permite actualizar los nombres de las ranuras en el chasis. Los nombres de las ranuras se utilizan para identificar a los 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*
 - *Alojamiento-Izquierdo*
 - *Alojamiento-Derecho*
 - *Alojamiento-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, debe tener privilegios de **Administrador de configuración del chasis**.



NOTA: El valor de los nombres de ranuras en la interfaz web reside en el CMC solamente. Si se quita un servidor del chasis, el valor del nombre de ranura no permanece con el servidor.



NOTA: El valor del nombre de ranura no se extiende al iKVM opcional. La información de nombre de ranura está disponible a través de la FRU del iKVM.



NOTA: El valor de los nombres de ranuras en la interfaz web del CMC siempre prevalece sobre cualquier cambio que usted aplique al nombre que aparece en la interfaz del iDRAC.

Para editar un nombre de ranura:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de servidores** en el menú **Chasis** del árbol del sistema.
- 3 Haga clic en **Configuración**→ **Nombres de ranuras**.
Aparecerá la página **Nombres de ranuras**.
- 4 Escriba el nombre nuevo o actualizado de la ranura en el campo **Nombre ranura**. Repita esta acción para cada ranura a la que desee cambiar el nombre y haga clic en **Aplicar**.
- 5 Para restablecer el nombre de ranura predeterminado (**SLOT-01** a **SLOT-16**, basándose en la ubicación de la ranura del servidor) al servidor, presione **Restaurar valor predeterminado**.

Uso del nombre de host del servidor como nombre de ranura

La página **Nombres de ranuras** permite reemplazar los nombres de ranuras estáticos por el nombre de host del servidor (o el nombre del sistema), si se encuentra disponible. Esto requiere que el agente OMSA esté instalado en el servidor. Para obtener más información sobre el agente OMSA, consulte la *Guía del usuario de Dell OpenManage Server Administrator*.

Para utilizar el nombre de host del servidor como nombre de ranura:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de servidores** en el menú **Chasis** del árbol del sistema.
- 3 Haga clic en **Configuración**→ **Nombres de ranuras**.
Aparecerá la página **Nombres de ranuras**.
- 4 Seleccione la casilla **Utilizar nombre de host para el nombre de ranura** y haga clic en **Aplicar**.

Cómo establecer el primer dispositivo de inicio para los servidores

La página **Primer dispositivo de inicio** le permite especificar el primer dispositivo de inicio del CMC para cada servidor. Es posible que este no sea el primer dispositivo de inicio real del servidor ni que represente un dispositivo presente en ese servidor si no que represente un dispositivo que el CMC utilizará como el primer dispositivo de inicio con respecto a ese servidor.

Puede definir el dispositivo de inicio predeterminado y también puede definir un dispositivo de inicio para una sola vez a fin de poder iniciar una imagen especial que realice tareas como ejecutar diagnósticos o reinstalar un sistema operativo.

El dispositivo de inicio que especifique debe existir y contener soportes iniciables.

Tabla 5-26. 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) está 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 está 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 RFS (Recurso compartido de archivos remotos). El archivo de imagen se adjunta con el visor de consola de la interfaz gráfica de usuario de iDRAC.



NOTA: Para configurar el primer dispositivo de inicio para los servidores, debe tener privilegios de **Administrador de servidor** o **Administrador de configuración del chasis** y **privilegios para iniciar sesión en el iDRAC**.

Para definir el primer dispositivo de inicio para algunos o todos los servidores del chasis:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Descripción general de servidores** en el árbol del sistema y, a continuación, haga clic en **Configuración** → **Primer dispositivo de inicio**. Se abre una lista de servidores.
- 3 Seleccione el dispositivo de inicio que desea utilizar para cada servidor en el cuadro de lista.
- 4 Si desea que el servidor utilice el dispositivo seleccionado cada vez que se inicia, deje en blanco la casilla **Inicio único**.
Si desea que el servidor utilice el dispositivo seleccionado solo en el siguiente ciclo de inicio, seleccione la casilla **Inicio único** para dicho servidor y haga clic en **Aplicar**.

Cómo ver el estado de la condición de un servidor individual

El estado de la condición de un servidor individual puede verse de dos maneras: Desde la sección **Gráficos del chasis** en la página **Condición del chasis** o en la página **Estado del servidor**.

La página **Condición del chasis** proporciona una descripción gráfica de un servidor individual instalado en el chasis.

Para ver el estado de la condición de los servidores individuales a través de **Gráficos del chasis**:

- 1 Inicie sesión en la interfaz web del CMC.
Aparecerá la página **Condición del chasis**. La sección superior de **Gráficos del chasis** muestra la vista frontal del chasis y contiene el estado de la condición de los servidores individuales. El estado de la condición del servidor se indica mediante la superposición de niveles del gráfico secundario del servidor:
 - Sin superposición: indica que el servidor está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - Señal de precaución de color ámbar: indica que solo se emitieron alertas de aviso y deben tomarse medidas correctivas.

- X de color rojo: indica que existe al menos una condición de falla. Esto significa que el CMC aún se puede comunicar con el componente y que el estado de la condición sobre la que se informa es crítico.
- Color gris: indica que el componente está presente y no está encendido. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.

2 Pase el cursor sobre el gráfico secundario de un servidor.

Aparecerá un cuadro de texto o una sugerencia de pantalla. El cuadro de texto proporciona información adicional sobre dicho servidor.

3 Haga clic en el gráfico secundario del servidor para seleccionar la información del servidor y ver los vínculos de acceso rápido a la derecha de los gráficos del chasis.

La página **Estado del servidor** (diferente a la página *Estado* de los servidores) proporciona una descripción general del servidor y un punto de inicio a la interfaz web para el Integrated Dell Remote Access Controller (iDRAC), que es el firmware que se utiliza para administrar el servidor.



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

Para ver el estado de la condición de un servidor individual:

- 1** Inicie sesión en la interfaz web del CMC.
- 2** Expanda la opción **Descripción general de servidores** en el árbol del sistema.

Todos los servidores (1 a 16) aparecen en la lista expandida de **Servidores**.

- 3** Haga clic en el servidor (ranura) que desea ver.

Se muestra la página **Estado del servidor**.

También puede visualizar la página Estado del servidor si hace clic en el vínculo de estado en los vínculos de acceso rápido del servidor que aparecen a la derecha de la página.

Tabla 5-27. Estado del servidor individual - Propiedades





Elemento	Descripción		
Ranura	Muestra la ranura ocupada por el servidor en el chasis. Los números de las ranuras son identificaciones progresivas, de 1 a 16 (hay 16 ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis.		
Nombre de ranura	Muestra el nombre de la ranura en la que reside el servidor.		
Presentación	Indica si el servidor está presente en la ranura (Sí o No). Cuando el servidor está ausente, se desconoce (no se muestra) la información sobre la condición, el estado de la alimentación y la etiqueta de servicio del servidor.		
Condición		En buen estado	Muestra que el servidor está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar el estado de la condición del servidor.
		Información	Muestra información acerca del servidor cuando no se ha producido ningún cambio en el estado de la condición (En buen estado, Advertencia, Crítico).
		Aviso	Muestra que solo se emitieron alertas de aviso y <i>que deben tomarse medidas correctivas</i> . Si no se toman medidas correctivas, existe la posibilidad de que surjan fallas críticas que pueden afectar la integridad del dispositivo.
		Crítico	Muestra que se ha enviado al menos una alerta de falla. El estado crítico representa una falla del sistema en el servidor y <i>se debe tomar acción correctiva inmediatamente</i> .
		Sin valor	Cuando el servidor no está presente en la ranura, no se proporciona información de su condición.

Tabla 5-27. Estado del servidor individual - Propiedades (continuación)

Elemento	Descripción
Modelo del servidor	Muestra el modelo del servidor en el chasis. Ejemplos: PowerEdge M600 o PowerEdge M605 .
Etiqueta de servicio	Muestra la etiqueta de servicio del servidor. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento. Si el servidor está ausente, este campo está vacío.
Firmware del iDRAC	Muestra la versión del iDRAC instalada actualmente en el servidor.
Versión de CPLD	Muestra el número de versión del dispositivo lógico programable complejo (CPLD) del servidor.
Versión del BIOS	Muestra la versión del BIOS en el servidor.
Sistema operativo	Muestra el sistema operativo en el servidor.
Información de CPU	Muestra el tipo u el número de CPU instaladas en el servidor.
Memoria total del sistema	Muestra la memoria total del sistema (en GB) instalada en el servidor.

Tabla 5-28. Estado del servidor individual - Registro de sucesos del sistema del iDRAC






Elemento	Descripción
Gravedad	 En buen estado Indica un suceso normal que no requiere acciones correctivas.
	 Información Indica una anotación informativa en un suceso en el que el estado de gravedad no ha cambiado.
	 Desconocido Indica un suceso desconocido o no categorizado.
	 Aviso Indica un suceso no crítico que requiere que se tomen acciones correctivas con prontitud a fin de evitar fallas del sistema.
	 Crítico Indica un suceso crítico que requiere de acciones correctivas inmediatas para evitar fallas del sistema.
Fecha/Hora	Muestra la fecha y hora exactas en la que ocurrió el suceso (por ejemplo, Miér 2 de mayo de 2007 16:26:55).
Descripción	Una breve descripción del suceso.

Tabla 5-29. Estado del servidor individual - Configuración de red del iDRAC

Elemento	Descripción
LAN activada	Indica si el canal LAN está activado (Sí) o desactivado (No).

Tabla 5-30. Estado del servidor individual - Configuración de red del iDRAC de IPv4

Elemento	Descripción
Activado	Indica si el protocolo IPv4 se utiliza en la LAN (Sí). Si el servidor no es compatible con IPv6, el protocolo IPv4 siempre está activado y esta configuración no se visualiza.
DHCP activado	Indica si Protocolo de configuración dinámica de host (DHCP) está activado (Sí) o desactivado (No). Si esta opción está seleccionada (Sí), el servidor recupera automáticamente la configuración de IP (dirección IP, máscara de subred y puerta de enlace) de un servidor DHCP en la red. El CMC siempre tiene asignada una dirección IP exclusiva en toda la red.
IPMI en LAN activado	Indica si el canal de LAN de IPMI está activado (Sí) o desactivado (No).
Dirección IP	Especifica la dirección IP para la interfaz de red del iDRAC.
Máscara de subred	Especifica la máscara de subred para la interfaz de red del iDRAC.
Puerta de enlace	Especifica la puerta de enlace para la interfaz de red del iDRAC.

Tabla 5-31. Estado del servidor individual - Configuración de red del iDRAC de IPv6

Elemento	Descripción
Activado	Indica si el protocolo IPv6 se utiliza en la LAN (Sí).
Configuración automática activada	Indica si la configuración automática para IPv6 está activada (Sí). Si la configuración automática está activada, el servidor recupera la configuración de IPv6 (Dirección IPv6 , Longitud del prefijo y Puerta de enlace IPv6) automáticamente de un enrutador IPv6 de su red. El servidor siempre tendrá una dirección IPv6 exclusiva en su red y podrá recibir hasta 16 direcciones IPv6.
Dirección local de vínculo	Dirección IPv6 asignada al CMC en base a la dirección MAC del CMC.
Puerta de enlace	Muestra la puerta de enlace IPv6 para la interfaz de red del iDRAC.
Dirección IPv6	Muestra una puerta de enlace IPv6 para la interfaz de red del iDRAC. Puede haber hasta 16 de estas direcciones. La longitud del prefijo, si es no cero, se expresa después de una diagonal ("/").

Tabla 5-32. Estado de servidor individual - Dirección de WWN/MAC

Elemento	Descripción
Ranura	Indica la ranura ocupada por el servidor en el chasis.
Ubicación	Muestra la ubicación ocupada por los módulos de entrada/salida. Las seis ubicaciones se identifican por una combinación del nombre del grupo (A, B o C) y el número de ranura (1 ó 2). Nombres de las ranuras: A1, A2, B1, B2, C1 o C2.
Red Fabric	Muestra el tipo de la red Fabric de E/S.
Asignada por el servidor	Muestra las direcciones WWN/MAC asignadas por el servidor integradas en el hardware de la controladora. Las direcciones WWN/MAC que muestran el texto N/A indican que no se ha instalado una interfaz para la red Fabric especificada.
Asignada por el chasis	Muestra las direcciones WWN/MAC asignadas por el chasis que se utilizan para la ranura particular. Las direcciones WWN/MAC que muestran el texto N/A indican que no se ha instalado la función FlexAddress. NOTA: Una marca verde en las columnas Asignadas por el servidor o Asignadas por el chasis indica el tipo de direcciones activas. NOTA: Cuando se activa FlexAddress, las ranuras sin servidores instalados muestra las direcciones WWN/MAC asignadas por el chasis para las controladoras Ethernet incorporadas (Red Fabric A). Las direcciones asignadas por el chasis para las redes Fabric B y C muestran N/A, a no ser que estas redes Fabric estén en uso en servidores en ranuras ocupadas; se asume que los mismos tipos de red Fabric serán instalados en las ranuras desocupadas.

Para obtener información acerca de cómo iniciar la consola de administración del iDRAC y políticas de inicio de sesión único, ver “Cómo iniciar el iDRAC mediante el inicio de sesión único” en la página 239.

Cómo ver la condición de los módulos de E/S

El estado de la condición de los módulos de E/S puede verse de dos maneras: Desde la sección **Resumen de componentes del chasis** en la página **Condición del chasis** o en la página **Estado de los módulos de E/S**. La página **Condición del chasis** ofrece una descripción gráfica de los módulos de E/S instalados en el chasis.

Para ver el estado de la condición de los módulos de E/S a través de Gráficos del chasis:

- 1 Inicie sesión en la interfaz web del CMC.

Aparecerá la página **Condición del chasis**. La sección inferior de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de la condición de los módulos de E/S. El estado de la condición del módulo de E/S se indica mediante la superposición de niveles del gráfico secundario del módulo de E/S:

- Sin superposición: el módulo de E/S está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
- Señal de precaución de color ámbar: indica que solo se emitieron alertas de aviso y deben tomarse medidas correctivas.
- X de color rojo: indica que existe al menos una condición de falla. Esto significa que el CMC aún se puede comunicar con el componente y que el estado de la condición sobre la que se informa es crítico.
- Color gris: indica que el módulo de E/S está presente y no está encendido. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.

- 2 Pase el cursor sobre el gráfico secundario de un módulo de E/S.

Aparecerá un cuadro de texto o una sugerencia de pantalla. El cuadro de texto proporciona información adicional sobre dicho módulo de E/S.

- 3 Haga clic en el gráfico secundario del módulo de E/S para seleccionar la información del módulo y los vínculos de acceso rápido que se muestran a la derecha de los gráficos del chasis.

La página **Estado de los módulos de E/S** proporciona descripciones generales de todos los módulos de E/S asociados con el chasis. Para obtener instrucciones acerca de cómo ver la condición de los módulos de E/S mediante la interfaz web o RACADM, ver “Supervisión de la condición del módulo de E/S” en la página 419.

Cómo ver el estado de la condición de los ventiladores



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

El estado de la condición de los ventiladores puede verse de dos maneras: desde la sección **Resumen de componentes del chasis** en la página **Condición del chasis** o en la página **Estado de los ventiladores**. La página **Condición del chasis** ofrece una descripción gráfica de todos los ventiladores instalados en el chasis.

Para ver el estado de la condición de todos los ventiladores a través de **Gráficos del chasis**:

1 Inicie sesión en la interfaz web del CMC.

Aparecerá la página **Condición del chasis**. La sección inferior de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de la condición de todos los ventiladores. El estado de la condición de los ventiladores se indica mediante la superposición de niveles del gráfico secundario de ventiladores:

- Sin superposición: el ventilador está presente y funcionando; no hay ninguna indicación sobre una condición adversa.
- Señal de precaución de color ámbar; indica que solo se emitieron alertas de aviso y deben tomarse medidas correctivas.
- X de color rojo; indica que existe al menos una condición de falla. Esto significa que el estado de la condición se reporta como crítico.
- Color gris; indica que el ventilador está presente y no está encendido. No existe una indicación de una condición adversa.

2 Pase el cursor sobre el gráfico secundario de un ventilador.

Aparecerá un cuadro de texto o una sugerencia de pantalla. El cuadro de texto proporciona información adicional sobre ese ventilador.

3 Haga clic en el gráfico secundario del ventilador para seleccionar la información del ventilador y los vínculos de acceso rápido que se muestran a la derecha de los gráficos del chasis.

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 más 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.

Para ver el estado de la condición de las unidades de ventilador:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Ventiladores** en el árbol del sistema.
Se muestra la página **Estado de los ventiladores**.

También puede ver la página **Estado de los ventiladores** si hace clic en el vínculo de estado en los vínculos de acceso rápido a información del ventilador a la derecha de la página.

Tabla 5-33. Información del estado de la condición de los ventiladores

Elemento	Descripción		
Nombre	Muestra el nombre del ventilador en el formato FAN-<i>n</i> , donde <i>n</i> es el número del ventilador.		
Presentación	Indica si la unidad del ventilador está presente (Sí o No).		
Condición		En buen estado	Indica que la unidad del ventilador está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el ventilador, el CMC no puede obtener ni mostrar el estado del ventilador.
		Crítico	Muestra que se ha enviado al menos una alerta de falla. Un estado crítico representa una falla del sistema en la unidad del ventilador y se debe realizar una acción correctiva inmediatamente para evitar el sobrecalentamiento y el apagado del sistema.
		Desconocido	Se muestra cuando el chasis se enciende por primera vez. En caso de una falla de comunicación entre el CMC y el ventilador, el CMC no puede obtener ni mostrar el estado del ventilador.
Velocidad	Indica la velocidad del ventilador en RPM.		

Cómo ver el estado 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. El estado de la condición del iKVM asociado con el chasis puede verse en la página **Condición del chasis**.

Para ver el estado del iKVM a través de **Gráficos del chasis**:

- 1 Inicie sesión en la interfaz web del CMC.

Aparecerá la página **Condición del chasis**. La sección inferior de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de la condición del iKVM. El estado de la condición del iKVM se indica mediante la superposición del gráfico secundario del iKVM:

- Sin superposición: el iKVM está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
- Señal de precaución de color ámbar: indica que solo se emitieron alertas de aviso y deben tomarse medidas correctivas.
- X de color rojo: indica que existe al menos una condición de falla. Esto significa que el CMC aún se puede comunicar con el iKVM y que el estado de la condición sobre la que se informa es crítico.
- Color gris: indica que el iKVM está presente y no está encendido. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.

- 2 Pase el cursor sobre el gráfico secundario de un iKVM.

Aparecerá un cuadro de texto o una sugerencia de pantalla. El cuadro de texto proporciona información adicional sobre ese iKVM.

- 3 Haga clic en el gráfico secundario del iKVM para seleccionar la información del iKVM y los vínculos de acceso rápido que se muestran a la derecha de los gráficos del chasis.

También puede visualizar la página **Estado de iKVM** si hace clic en el vínculo de estado en los vínculos de acceso rápido de iKVM que aparecen a la derecha de la página.

Para obtener instrucciones adicionales acerca de cómo ver el estado y las propiedades de configuración del iKVM, ver:

- “Cómo ver el estado y las propiedades del iKVM” en la página 407
- “Activación o desactivación del panel anterior” en la página 406
- “Activación de la consola de CMC de Dell a través de iKVM” en la página 407
- “Actualización del firmware de iKVM” en la página 409

Para obtener más información acerca del iKVM, ver “Uso del módulo iKVM” en la página 387.

Cómo ver el estado de la condición de las unidades de suministro de energía

El estado de la condición de las unidades de suministro de energía relacionadas con el chasis puede verse de dos maneras: desde la sección **Resumen de componentes del chasis** en la página **Condición del chasis** o en la página **Estado del suministro de energía**. La página **Condición del chasis** ofrece una descripción gráfica de todas las unidades de suministro de energía instaladas en el chasis.

Para ver el estado de la condición de todas las unidades de suministro de energía a través de **Gráficos del chasis**:

- 1 Inicie sesión en la interfaz web del CMC.

Aparecerá la página **Condición del chasis**. La sección inferior de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de la condición de todas las unidades de suministro de energía. El estado de la condición de la unidad de suministro de energía se indica mediante la superposición del gráfico secundario de la unidad:

- Sin superposición: la unidad de suministro de energía está presente, encendida y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
- Señal de precaución de color ámbar: indica que solo se emitieron alertas de aviso y deben tomarse medidas correctivas.
- X de color rojo: indica que existe al menos una condición de falla. Esto significa que el CMC aún se puede comunicar con la unidad de suministro de energía y que el estado de la condición sobre la que se informa es crítico.
- Color gris: indica que la unidad de suministro de energía está presente y no está encendida. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.

- 2 Al pasar el cursor sobre el gráfico secundario de una unidad de suministro de energía individual se mostrará un cuadro de texto o una sugerencia de pantalla. El cuadro de texto proporciona información adicional sobre esa unidad de suministro de energía.
- 3 Haga clic en el gráfico secundario de la unidad de suministro de energía para seleccionar la información de la unidad y los vínculos de acceso rápido que se muestran a la derecha de los gráficos del chasis.

La página **Estado del suministro de energía** muestra el estado y las lecturas de las unidades de suministro de energía asociadas con el chasis. Para obtener más información acerca de la administración de la alimentación en el CMC, ver “Administración de la alimentación” en la página 333.

Para ver el estado de la condición de las unidades de suministro de energía:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Suministros de energía** en el árbol del sistema.

Se muestra la página **Estado de la unidad de suministro de energía**.

También puede visualizar la página **Estado de la unidad de suministro de energía** si hace clic en el vínculo de estado en los vínculos de acceso rápido de la unidad que aparecen a la derecha de la página.

Tabla 5-34. Información del estado de la condición del suministro de energía


Elemento	Descripción	
Nombre	Muestra el nombre de la unidad de suministro de energía: <i>PS-n</i> , donde <i>n</i> es el número del suministro de energía.	
Presentación	Indica si el suministro de energía está presente (Sí o No).	
Condición	 En buen estado	Indica que la unidad de suministro de energía está presente y se está comunicando con el CMC. Indica que la unidad de suministro de energía se encuentra en buen estado. En caso de una falla de comunicación entre el CMC y el ventilador, el CMC no puede obtener ni mostrar el estado de la unidad de suministro de energía.

Tabla 5-34. Información del estado de la condición del suministro de energía



Elemento	Descripción
 Crítico	Indica que la unidad de suministro de energía tiene una falla y su condición es crítica. Se debe ejecutar una acción correctiva inmediatamente. Si no lo hace, puede provocar que el componente se apague como consecuencia de una pérdida de alimentación.
 Desconocido	Se muestra cuando el chasis se enciende por primera vez. En caso de una falla de comunicación entre el CMC y la unidad de suministro de energía, el CMC no puede obtener ni mostrar el estado de la unidad de suministro de energía.
Estado de la alimentación	Indica el estado de la alimentación de la unidad de suministro de energía: En línea, Apagado o Ranura vacía.
Capacidad	Muestra la capacidad de alimentación en vatios.

Tabla 5-35. Estado de alimentación del sistema

Elemento	Descripción
Condición general de la alimentación	Muestra el estado de la condición (En buen estado, No crítico, Crítico, No recuperable, Otro, Desconocido) de la administración de la alimentación de todo el chasis.
Estado de alimentación del sistema	Muestra el estado de la alimentación (Encendido, Apagado, Encendiéndose, Apagándose) del chasis.
Redundancia	Muestra el estado de redundancia del suministro de energía. Los valores incluyen: No: los suministros de energía no son redundantes. Sí: hay redundancia total.

Cómo ver el estado de los sensores de temperatura

La página **Estado de sensores de temperatura** muestra el estado y la lectura de las sondas de temperatura de todo el chasis (chasis y servidores).







NOTA: El valor de las sondas de temperatura no se puede editar. Cualquier cambio que sobrepase el umbral provocará una alerta que hará que varíe la velocidad del ventilador. Por ejemplo, si la sonda de temperatura ambiente del CMC excede el umbral, la velocidad de los ventiladores del chasis aumentará.

Para ver el estado de la condición de las sondas de temperatura:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Sensores de temperatura** en el árbol del sistema.
Aparecerá la página **Estado de Sensores de temperatura**.

Tabla 5-36. Información del estado de la condición de los sensores de temperatura

Elemento	Descripción		
Id.	Muestra la ubicación de la sonda de temperatura.		
Nombre	Muestra el nombre de cada sonda de temperatura del chasis y los servidores.		
Presentación	Indica si el módulo está presente (Sí) o ausente (No) en el chasis.		
Condición		En buen estado	Indica que la unidad de suministro de energía está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar el estado de la condición del servidor.
		Aviso	Muestra que solo se emitieron alertas de aviso y que deben tomarse medidas correctivas. Si no se toman medidas correctivas, existe la posibilidad de que surjan fallas críticas que pueden afectar la integridad del módulo.
		Grave	Muestra que se ha enviado una alerta de falla. El estado crítico representa una falla del sistema en el módulo y se debe tomar una acción correctiva inmediatamente.
		Desconocido	Indica que no se ha establecido comunicación con el módulo. Usualmente, esto se debe a que el chasis está apagado o no ha completado la inicialización.
Lectura	Muestra la temperatura actual en grados centígrados y Fahrenheit.		
Umbral máximo	Muestra la temperatura más alta, en grados centígrados y Fahrenheit, a la que se emite una alerta de error.		

Visualización del estado de la pantalla LCD

Puede ver el estado de la condición de la pantalla LCD por medio de los gráficos del chasis relacionados en la página **Condición del chasis**.

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

- 1 Inicie sesión en la interfaz web del CMC.

Aparecerá la página **Condición del chasis**. La sección superior de Gráficos del chasis muestra la vista frontal del chasis. El estado de la condición de la pantalla LCD se indica mediante la superposición del gráfico secundario de la pantalla LCD:

- Sin superposición: la pantalla LCD está presente y encendida, y se está comunicando con el CMC. No existe una condición adversa.
 - Señal de precaución de color ámbar: se emitieron alertas de aviso y deben tomarse medidas correctivas.
 - X de color rojo: indica que existe al menos una condición de falla. El estado de la condición es crítico.
 - Color gris: indica que la pantalla LCD está presente y no está encendida. No se está comunicando con el CMC y no hay ninguna una condición adversa.
- 2 Pase el cursor sobre el gráfico secundario de la pantalla LCD. Aparecerá un cuadro de texto o una sugerencia de pantalla con información adicional sobre la pantalla LCD.
 - 3 Haga clic en el gráfico secundario de la pantalla LCD para seleccionar la información correspondiente y visualizarla a la derecha de los gráficos del chasis.

Cómo ver las identificaciones World Wide Name/Media Access Control (WWN/MAC)

La página Resumen de WWN/MAC le permite ver la configuración 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: Ver “Uso de FlexAddress” en la página 257 para obtener más información acerca de la función FlexAddress.

Direcciones WWN/MAC


La sección **Dirección WWN/MAC** muestra la información de WWN/MAC que se asigna a todos los servidores, aun si esas ranuras de servidor se encuentren actualmente vacías. **Ubicación** muestra la ubicación de la ranura ocupada por los módulos de entrada/salida. Las seis ranuras se identifican por una combinación del nombre de grupo (A, B o C) y el número de ranura (1 ó 2): Nombres de las ranuras A1, A2, B1, B2, C1 o C2. iDRAC es la controladora de administración integrado 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 específica. 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 aun que se sustituya un servidor por otro servidor.

Configuración de las propiedades de red del CMC

 **NOTA:** Los cambios de la configuración de la red pueden ocasionar la pérdida de conectividad en el inicio de sesión de red actual.


Configuración del acceso inicial al CMC


Antes de que pueda comenzar a configurar el CMC, debe establecer primero la configuración de red del CMC para permitir la administración remota del CMC. Esta configuración inicial asigna los parámetros del sistema de red TCP/IP que permiten tener acceso al CMC.


 **NOTA:** Debe tener privilegios de **Administrador de configuración del chasis** para configurar los valores de red del CMC.

- 1 Inicie sesión en la interfaz web.
- 2 Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Red**.
Aparecerá la página **Configuración de red**.
- 4 Active o desactive DHCP para el CMC seleccionando o dejando en blanco la casilla **Usar DHCP** (para la dirección IP de interfaz de red del CMC).
- 5 Si desactivó el DHCP, escriba la dirección IP, la puerta de enlace y la máscara de subred.
- 6 Haga clic en **Aplicar cambios** en la parte inferior de la página.

Configuración de los valores de red de la LAN

 **NOTA:** Debe tener privilegios de **Administrador de configuración del chasis** para configurar los valores de red del CMC.

 **NOTA:** Los valores en la página **Configuración de la red**, como la cadena de comunidad y la dirección IP del servidor SMTP, afectan tanto al CMC como a la configuración externa del chasis.

 **NOTA:** Si tiene dos CMC (activo y en espera) en el chasis y están conectados a la red, el CMC en espera asumirá automáticamente la configuración de la red en caso que el CMC activo falle.

Para configurar la LAN de red siga los pasos siguientes:

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Red**.
- 3 Establezca la configuración de red del CMC descrita en Tabla 5-37 a través de Tabla 5-39 y haga clic en **Aplicar cambios**.

Para configurar los valores de rango de IP y bloqueo de IP, haga clic en el botón **Configuración avanzada** (ver “Configuración de los valores de seguridad de la red del CMC” en la página 170).

Para actualizar el contenido de la página **Configuración de la red**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Configuración de la red**, haga clic en **Imprimir**.

Tabla 5-37. Configuración de red

Valor	Descripción
Dirección MAC del CMC	Muestra la dirección MAC del chasis, que es un identificador único del chasis en toda la red de equipos.
Activar la interfaz de red de CMC	<p>Activa la interfaz de red del CMC.</p> <p>Valor predeterminado: activado. Si esta opción está seleccionada:</p> <ul style="list-style-type: none"> • El CMC se comunicará con la red de equipos y se podrá acceder al mismo mediante ella. • La interfaz web, la CLI (RACADM remoto), WSMAN, Telnet y SSH relacionados con el CMC están disponibles. <p>Si esta opción no está seleccionada:</p> <ul style="list-style-type: none"> • La interfaz de red del CMC no podrá establecer comunicación a través de la red. • La comunicación con el chasis a través del CMC no estará disponible. • La interfaz web, la CLI (RACADM remoto), WSMAN, Telnet y SSH relacionados con el CMC no estarán disponibles. • La interfaz web del iDRAC del servidor, la CLI local, los módulos de E/S y el iKVM seguirán estando disponibles. • Las direcciones de red del iDRAC y el CMC se podrán obtener, en este caso, de la pantalla LCD del chasis. <p>NOTA: El acceso a los otros componentes accesibles mediante la red en el chasis no se afecta cuando la red en el chasis se desactiva (o se pierde).</p>

Tabla 5-37. Configuración de red (continuación)

Valor	Descripción
Registrar el CMC en DNS	<p>Esta propiedad registra el nombre del CMC en el servidor DNS.</p> <p>Valor predeterminado: sin seleccionar (desactivado) de manera predeterminada.</p> <p>NOTA: Algunos de los servidores DNS solo registran nombres de 31 caracteres o menos. Asegúrese de que el nombre designado esté dentro del límite requerido por DNS.</p>
Nombre DNS del CMC	<p>Muestra el nombre del CMC únicamente cuando la opción Registrar el CMC en DNS está seleccionada. El nombre predeterminado del CMC es <i>CMC_service_tag</i>, donde <i>service tag</i> es la etiqueta de servicio del chasis, por ejemplo: CMC-00002. El número máximo de caracteres es 63. El primer carácter debe ser una letra (a-z, A-Z), seguida de un carácter alfanumérico (a-z, A-Z, 0-9) o de un guión (-).</p>
Utiliza DHCP para el nombre del dominio de DNS	<p>Utiliza el nombre del dominio DNS predeterminado. Esta casilla solo se activa cuando la opción Usar DHCP (para la dirección IP de la interfaz de red del CMC) está seleccionada.</p> <p>Valor predeterminado: activado.</p>
Nombre de dominio de DNS	<p>El nombre predeterminado del dominio DNS es un carácter en blanco. Este campo solo se puede editar cuando la casilla Usar DHCP para el nombre del dominio DNS está seleccionada.</p>
Negociación automática (1 Gb)	<p>Determina si el CMC establece automáticamente el modo dúplex y la velocidad de la red por medio de la comunicación con el enrutador o conmutador más cercano (Encendido), o le permite establecer el modo dúplex y la velocidad de la red manualmente (Apagado).</p> <p>Valor predeterminado: encendido.</p> <p>Si la negociación automática está activada, el CMC se comunica automáticamente con el enrutador o conmutador más cercano o cambia y funciona a la velocidad de 1 Gb.</p> <p>Si la negociación automática está desactivada, usted deberá establecer manualmente el modo dúplex y la velocidad de la red.</p>

Tabla 5-37. Configuración de red (continuación)

Valor	Descripción
Velocidad de la red	<p>Establezca el valor de la velocidad de la red en 100 Mbps o 10 Mbps para que coincida con el entorno de la red.</p> <p>NOTA: Para que el rendimiento de la red sea efectivo, el valor de Velocidad de la red deberá 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 aumentará y la comunicación por medio de la red se hará 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 utilizar la opción Negociación automática o consultar al fabricante del equipo de red.</p> <p>NOTA: Para utilizar velocidades de 1000 Mb o 1 Gb, seleccione Negociación automática.</p>
Modo dúplex	<p>Establezca el valor del modo dúplex en completo o medio para que coincida con el entorno de la red.</p> <p>Implicaciones: si la Negociación automática está activada para un dispositivo pero no para otro, el dispositivo que esté utilizando la negociación automática podrá determinar la velocidad de la red del otro dispositivo, pero no el modo dúplex. En este caso, el modo dúplex se predetermina a la configuración de medio dúplex durante la negociación automática. Esta incompatibilidad de la configuración de dúplex hará que la conexión de red sea lenta.</p> <p>NOTA: Los valores de la velocidad de la red y del modo dúplex no están disponibles si la negociación automática está activada.</p>
MTU	<p>Establece el tamaño de la unidad de transmisión máxima (MTU) o el paquete más grande que se puede transferir por la interfaz.</p> <p>Rango de configuración: De 576 a 1500.</p> <p>Valor predeterminado: 1500.</p> <p>NOTA: IPv6 requiere una MTU mínima de 1280. Si IPv6 está activado y cfgNetTuningMtu tiene un valor menor, el CMC utilizará una MTU de 1.280.</p>

Tabla 5-38. Configuración de IPv4

Valor	Descripción
Activar IPv4	<p>Permitir que el CMC utilice el protocolo IPv4 para comunicarse en la red. Deseleccionar esta casilla no impide que ocurra la conexión en red de IPv6.</p> <p>Valor predeterminado: seleccionado (activado)</p>
Activar DHCP	<p>Permite que el CMC solicite y obtenga automáticamente una dirección IP del servidor de protocolo de configuración dinámica de host (DHCP) IPv4.</p> <p>Valor predeterminado: seleccionado (activado)</p> <p>Si esta opción está seleccionada, el CMC recupera automáticamente la configuración de IPv4 (dirección IP, máscara de subred y puerta de enlace) de un servidor DHCP de su red. El CMC siempre tiene asignada una dirección IP exclusiva en toda la red.</p> <p>NOTA: Cuando esta función está activada, los campos de propiedad Dirección IP estática, Máscara de subred estática y Puerta de enlace estática (que se encuentran inmediatamente después de esta opción en la página Configuración de la red) se desactivan, y todos los valores introducidos previamente para estas propiedades se ignoran.</p> <p>Si no se selecciona esta opción, deberá escribir manualmente la Dirección IP estática, la Máscara de subred estática y la Puerta de enlace estática en los campos de texto que se encuentran inmediatamente después de esta opción en la página Configuración de la red.</p>
Dirección IP estática	<p>Especifica la dirección IPv4 para la interfaz de red del CMC.</p>
Máscara de subred estática	<p>Especifica la máscara de subred estática IPv4 para la interfaz de red del CMC.</p>

Tabla 5-38. Configuración de IPv4 (continuación)

Valor	Descripción
Puerta de enlace estática	<p>Especifica la puerta de enlace IPv4 para la interfaz de red del CMC.</p> <p>NOTA: Los campos Dirección IP estática, Máscara de subred estática y Puerta de enlace estática se encuentran activos solamente si Activar DHCP (el campo de propiedad que precede a estos campos) está desactivado (deseleccionado). En tal caso, deberá escribir manualmente la Dirección IP estática, la Máscara de subred estática y la Puerta de enlace estática que el CMC debe utilizar en la red.</p> <p>NOTA: Los campos Dirección IP estática, Máscara de subred estática y Puerta de enlace estática corresponden únicamente al dispositivo del chasis. No afectan a los otros componentes accesibles a través de la red en la solución del chasis, como la red de servidores, el acceso local, los módulos de E/S y el iKVM.</p>
Usar DHCP para obtener direcciones de servidor DNS	<p>Obtiene las direcciones primaria y secundaria del servidor DNS a partir del servidor DHCP en vez de utilizar los valores estáticos.</p> <p>Valor predeterminado: seleccionado (activado) de manera predeterminada</p> <p>NOTA: Si la opción Usar DHCP (para la dirección IP de la interfaz de red del CMC) está activada, active la propiedad Usar DHCP para obtener direcciones de servidor DNS.</p> <p>Si esta opción está seleccionada, el CMC recupera automáticamente la dirección IP de DNS a partir del servidor DHCP de la red.</p> <p>NOTA: Cuando esta propiedad está activada, los campos de propiedades Servidor DNS preferido estático y Servidor DNS alternativo estático (que se encuentran inmediatamente después de esta opción en la página Configuración de la red) se desactivan y todos los valores que se hayan introducido anteriormente para estas propiedades se ignoran.</p> <p>Si la opción no está seleccionada, el CMC obtendrá la dirección IP del DNS del servidor DNS preferido estático y del servidor DNS alternativo estático. Las direcciones de estos servidores se especifican en los campos de texto que están inmediatamente después en la página Configuración de la red.</p>

Tabla 5-38. Configuración de IPv4 (continuación)

Valor	Descripción
Servidor DNS preferido estático	Especifica la dirección IP estática del servidor DNS preferido. El servidor DNS preferido estático se implementa solo cuando la opción Usar DHCP para obtener direcciones del servidor DNS está desactivada.
Servidor DNS alternativo estático	Especifica la dirección IP estática del servidor DNS alternativo. El servidor DNS alternativo estático se implementa solo cuando la opción Usar DHCP para obtener direcciones del servidor DNS está desactivada. Si no tiene un servidor DNS alternativo, introduzca una dirección IP de 0.0.0.0.

Tabla 5-39. Configuración de IPv6

Valor	Descripción
Activar IPv6	Permite que el CMC utilice el protocolo IPv6 para comunicarse en la red. Deseleccionar esta casilla no impide que ocurra la conexión en red de IPv4. Valor predeterminado: seleccionado (activado)
Activar configuración automática	Permite al CMC utilizar el protocolo IPv6 para obtener parámetros de dirección y puerta de enlace relacionados con IPv6 de un enrutador IPv6 configurado para proporcionar esta información. Entonces el CMC dispondrá de una dirección IPv6 exclusiva en su red. Valor predeterminado: seleccionado (activado) NOTA: Cuando esta función está activada, los campos de propiedad Dirección IPv6 estática , Longitud de prefijo estática y Puerta de enlace estática (que se encuentran inmediatamente después de esta opción en la página Configuración de la red) se desactivan, y todos los valores introducidos previamente para estas propiedades se ignoran. Si esta opción no se selecciona, deberá escribir manualmente la dirección IPv6 estática, la longitud de prefijo estática y la puerta de enlace estática en los campos de texto que se encuentran inmediatamente después de esta opción en la página Configuración de la red .
Dirección IPv6 estática	Especifica la dirección IPv6 para la interfaz de red del CMC cuando no está activada la configuración automática.

Tabla 5-39. Configuración de IPv6 (continuación)

Valor	Descripción
Longitud de prefijo estática	Especifica la longitud del prefijo IPv6 para la interfaz de red del CMC cuando no está activada la configuración automática.
Puerta de enlace estática	Especifica la puerta de enlace IPv6 estática para la interfaz de red del CMC cuando no está activada la configuración automática. NOTA: Los campos Dirección IPv6 estática , Longitud de prefijo estática y Puerta de enlace estática se encuentran activos solamente si Activar configuración automática (el campo de propiedad que precede a estos campos) está desactivado (deseleccionado). En tal caso, deberá escribir manualmente la Dirección IPv6 estática , la Longitud de prefijo estática y la Puerta de enlace estática que el CMC debe utilizar en la red IPv6. NOTA: Los campos Dirección IPv6 estática , Longitud de prefijo estática y Puerta de enlace estática corresponden únicamente al dispositivo del chasis. No afectan a los otros componentes accesibles a través de la red en la solución del chasis, como la red de servidores, el acceso local, los módulos de E/S y el iKVM.
Servidor DNS preferido estático	Especifica la dirección IPv6 estática del servidor DNS preferido. El valor del servidor DNS preferido estático solamente se considera cuando Usar DHCP para obtener direcciones de servidor DNS está desactivada o deseleccionada. Existe un valor para este servidor en las áreas de configuración de IPv4 e IPv6.
Servidor DNS alternativo estático	Especifica la dirección IPv6 estática del servidor DNS alternativo. Si no tiene un servidor DNS alternativo, escriba una dirección IPv6 de “::”. El valor del servidor DNS alternativo estático solamente se considera cuando Usar DHCP para obtener direcciones de servidor DNS está desactivada o deseleccionada. Existe un valor para este servidor en las áreas de configuración de IPv4 e IPv6.

Configuración de los valores de seguridad de la red del CMC



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

Para configurar los valores de seguridad de la red del CMC.

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Red**.
Aparecerá la página **Configuración de la red**.
- 3 Haga clic en el botón **Configuración avanzada**.
Aparecerá la página **Seguridad de la red**.
- 4 Configure los valores de seguridad de la red del CMC.
La Tabla 5-40 describe los valores de la página **Seguridad de la red**.



NOTA: Los valores de Rango de IP y Bloqueo de IP se aplican únicamente a IPv4.

Tabla 5-40. Valores de la página de seguridad de la red

Configuración	Descripción
Rango de IP activado	Activa la función de verificación del rango IP, que define un rango específico de direcciones IP que pueden acceder al CMC.
Dirección del rango de IP	Determina la dirección IP de base para la verificación del rango.
Máscara de rango de IP	Define un rango específico de direcciones IP que pueden acceder al CMC, un proceso que se denomina verificación de rango de IP. La verificación de rango de IP permite el acceso al CMC solo desde clientes o estaciones de administración cuyas direcciones IP están dentro del rango definido por el usuario. Los demás inicios de sesión se rechazan. Por ejemplo: Máscara de rango de IP: 255.255.255.0 (11111111.11111111.11111111.00000000) Dirección de rango de IP: 192.168.0.255 (11000000.10101000.00000000.11111111) El rango de dirección IP resultante es cualquier dirección que contenga 192.168.0, es decir, cualquier dirección entre 192.168.0.0 y 192.168.0.255.

Tabla 5-40. Valores de la página de seguridad de la red (continuación)

Configuración	Descripción
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo preestablecido.
Número de fallas de bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección.
Ventana de fallas de bloqueo de IP	Determina el periodo en segundos dentro de cual se debe producir el número de fallas de bloqueo de IP para iniciar el tiempo de penalización de bloqueo IP.
Tiempo de penalización de bloqueo de IP	El periodo en segundos dentro del que se rechazan los intentos de inicio de sesión que provengan de una dirección IP que ha tenido un número excesivo de intentos fallidos. NOTA: Los campos Número de fallas de bloqueo de IP , Ventana de fallas de bloqueo de IP y Tiempo de penalización de bloqueo de IP están activos solo si la casilla Bloqueo de IP activado (el campo de propiedad que precede a estos campos) está seleccionada (activada). En ese caso, debe escribir manualmente las propiedades Número de fallas de bloqueo de IP , Ventana de fallas de bloqueo de IP y Tiempo de penalización de bloqueo de IP .

- 5 Haga clic en **Aplicar** para guardar la configuración.

Para actualizar el contenido de la página **Seguridad de la red**, haga clic en **Actualizar**. Para imprimir el contenido de la página **Seguridad de la red**, haga clic en **Imprimir**.

Configuración de VLAN

Las VLAN se utilizan para permitir que diferentes 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. Para configurar VLAN:

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Red** → subficha **VLAN**.
Aparecerá la página **Configuración de etiquetas VLAN**. Las etiquetas VLAN son propiedades del chasis. Se conservan con el chasis aunque se quite el componente.
- 3 Configure los valores de VLAN del CMC/iDRAC.

La Tabla 5-41 describe los valores de la página Seguridad de la red.

Tabla 5-41. Configuración de etiquetas VLAN

Valor	Descripción
Ranura	Muestra la ranura ocupada por el servidor en el chasis. Las ranuras son identificaciones consecutivas, de 1 a 16 (de las 16 ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis.
Nombre	Muestra el nombre del servidor en cada ranura.
Activar	Activa VLAN si la casilla está seleccionada. De forma predeterminada, VLAN está desactivada.
Prioridad	Indica el nivel de prioridad de tramas, que se puede utilizar para priorizar distintos tipos de tráfico (voz, video y datos). Las prioridades válidas son de 0 a 7; donde 0 (predeterminado) es la menor y 7 la mayor.
Id.	Muestra la identificación de VLAN. Las identificaciones de VLAN válidas son: 1 a 4000 y 4021 a 4094. La identificación de VLAN predeterminada es 1.

4 Haga clic en **Aplicar** para guardar los valores.

También puede acceder a esta página a través de **Descripción general del chasis**→ **Servidores**→ ficha **Configuración**→ subficha **VLAN**.

Cómo agregar y configurar usuarios del CMC

Para administrar el sistema con el CMC y mantener la seguridad del sistema, cree usuarios únicos con permisos administrativos específicos (o *con autoridad basada en funciones*). Para obtener seguridad adicional, también puede configurar alertas que se envían por correo electrónico a usuarios específicos cuando ocurre un suceso determinado en el sistema.

Tipos de usuarios

Hay dos tipos de usuarios: usuarios del CMC y usuarios del iDRAC. Los usuarios del CMC también se conocen como “usuarios del chasis”. Como el iDRAC reside en el servidor, los usuarios del iDRAC se conocen como “usuarios del servidor”.

Los usuarios del CMC pueden ser usuarios locales o usuarios del servicio de directorio. Los usuarios del iDRAC también pueden ser usuarios locales o del servicio de directorio.

Excepto cuando un usuario del CMC tiene privilegios de **Administrador de servidor**, los privilegios otorgados a los usuarios 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 servidor desde CMC ni viceversa. Esta regla protege la seguridad y la integridad de los servidores.

Tabla 5-42. Tipos de usuarios

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

Tabla 5-42. Tipos de usuarios (continuación)

Privilegio	Descripción
Administrador de configuración del chasis	<p>El usuario puede agregar o cambiar los datos que:</p> <ul style="list-style-type: none"> • Identifican el chasis, como el nombre del chasis y la ubicación de este. • 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. • Proporcionan servicios al chasis, como la fecha y la hora, la actualización del firmware y el restablecimiento del CMC. • Se relacionan con el chasis, como el nombre de ranura y la prioridad de ranuras. 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 de las ranuras y sus prioridades se pueden agregar o cambiar sin importar si los servidores están presentes en las ranuras. <p>Cuando un servidor se cambia a otro chasis, hereda el nombre de ranura y la prioridad asignada a la ranura que ocupe en el nuevo chasis. El nombre y la prioridad de ranura anteriores se quedarán en el chasis anterior.</p> <p>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.</p>
Administrador de configuración de usuarios	<p>El usuario puede:</p> <ul style="list-style-type: none"> • Agregar un nuevo usuario. • Eliminar un usuario existente. • Cambiar la contraseña de un usuario. • Cambiar los privilegios de un usuario. • Activar o desactivar el privilegio de inicio de sesión del usuario, pero conservar el nombre del usuario y otros privilegios en la base de datos.
Administrador de borrado de registros	<p>El usuario puede borrar los registros de hardware y de CMC.</p>

Tabla 5-42. Tipos de usuarios (continuación)

Privilegio	Descripción
Administrador de control del chasis (Comandos de alimentación)	<p>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 operaciones de alimentación del chasis, como el encendido, el apagado y el ciclo de encendido.</p> <p>NOTA: Para configurar los valores de alimentación, es necesario el privilegio de Administrador de configuración del chasis.</p>
Server Administrator	<p>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.</p> <p>Cuando un usuario con privilegios de Administrador del servidor genera una acción que se va a 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 Administrador del servidor anula la falta de privilegios de administrador en el servidor.</p> <p>Sin el privilegio de Administrador del servidor, los usuarios que hayan sido creados en el chasis solo pueden ejecutar un comando en un servidor cuando se cumplan todas las condiciones siguientes:</p> <ul style="list-style-type: none">• 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. <p>Cuando un usuario del CMC que no tiene privilegios de Administrador del servidor genera una acción que se va a ejecutar en un servidor, el CMC envía un comando al servidor de destino con el nombre de inicio de sesión y la contraseña del usuario. Si el usuario no existe en el servidor o si la contraseña no coincide, se negará al usuario la capacidad de ejecutar la acción.</p> <p>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 a ejecutar la acción.</p>

Tabla 5-42. Tipos de usuarios (continuación)

Privilegio	Descripción
	<p>A continuación se muestra una lista de los privilegios y acciones en el servidor a los que se tiene derecho con el privilegio de Administrador del servidor. Estos derechos se aplican únicamente cuando el usuario del chasis no tiene privilegios de Administrador del servidor en el chasis.</p>
<p>Administrador del servidor (continuación)</p>	<p>Administrador de configuración del servidor:</p> <ul style="list-style-type: none"> • Establecer dirección IP • Establecer puerta de enlace • Establecer máscara de subred • Establecer primer dispositivo de inicio <p>Configurar usuarios:</p> <ul style="list-style-type: none"> • Establecer contraseña raíz de iDRAC • Restablecimiento de iDRAC <p>Administrador de control del servidor:</p> <ul style="list-style-type: none"> • Encendido • Alimentación apagada • Ciclo de encendido • Apagado ordenado • Reinicio del servidor
<p>Usuario de alertas de prueba</p>	<p>El usuario puede enviar mensajes de alerta.</p>
<p>Administrador de comandos de depuración</p>	<p>El usuario puede ejecutar comandos de diagnóstico del sistema.</p>
<p>Administrador de red Fabric A</p>	<p>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.</p>
<p>Administrador de red Fabric B</p>	<p>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.</p>

Tabla 5-42. Tipos de usuarios (continuación)

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.
Superusuario	El usuario cuenta con acceso raíz al CMC y tiene privilegios de Administrador de configuración de usuarios y Inicio de sesión con el usuario del CMC . Solo los usuarios con privilegios de Superusuario pueden otorgar a los usuarios nuevos o ya existentes privilegios de Administrador de comandos de depuración y Superusuario .

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 luego agrega o elimina un privilegio del conjunto predefinido, el grupo del CMC cambiará automáticamente a **Personalizado**.

Tabla 5-43. Privilegios del grupo del CMC

Grupo de usuarios	Privilegios otorgados
Administrador	<ul style="list-style-type: none">• 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

Tabla 5-43. Privilegios del grupo del CMC (continuación)

Grupo de usuarios	Privilegios otorgados
Usuario avanzado	<ul style="list-style-type: none">• Inicio de sesión• Administrador de borrado de registros• Administrador de control del chasis• 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
Personalizar	Selección de cualquier combinación de los siguientes permisos: <ul style="list-style-type: none">• 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• Superusuario• 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
Ninguno	Sin permisos asignados

Tabla 5-44. Comparación de los privilegios entre administradores, usuarios avanzados y usuarios invitados del CMC

Conjunto de privilegios	Permisos de administrador	Usuario avanzado Permisos	Usuario invitado 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	✓	✓	✗
Superusuario	✓	✗	✗
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	✓	✓	✗

Cómo agregar y administrar usuarios

En las páginas **Usuarios** y **Configuración de usuarios** en la interfaz web, usted puede ver información acerca de los usuarios del CMC, agregar un nuevo usuario y cambiar la configuración de un usuario existente.

Puede configurar hasta 16 usuarios locales. Si se requieren usuarios adicionales y la empresa utiliza Microsoft Active Directory o los servicios genéricos del Protocolo ligero de acceso a directorios (LDAP), puede definir la configuración para proporcionar acceso al CMC. La configuración de Active Directory le permite agregar y controlar privilegios de usuarios del CMC para sus usuarios existentes en el software de Active Directory, además de los 16 usuarios locales. Para obtener más información, consulte “Uso del servicio de directorio del CMC” en la página 281. Para obtener más información sobre el protocolo LDAP, consulte la sección “Uso de CMC con servicios de protocolo ligero de acceso a directorios”.

Los usuarios se pueden conectar mediante sesiones de la interfaz web, Telnet serie, SSH e iKVM. Se puede dividir un máximo de 22 sesiones activas (interfaz web, Telnet, serie, SSH e iKVM, en cualquier combinación) entre los usuarios.



NOTA: Para mayor seguridad, se recomienda cambiar la contraseña predeterminada de la cuenta raíz (usuario 1). La cuenta raíz es la cuenta administrativa predeterminada que se incluye con el CMC. Para cambiar la contraseña predeterminada de la cuenta raíz, haga clic en **Id. de usuario 1** para abrir la página **Configuración de usuario**. La ayuda para esa página está disponible mediante el vínculo **Ayuda** en la esquina superior derecha de la página.

Para agregar y configurar usuarios del CMC:



NOTA: Para poder realizar los pasos a continuación, debe tener privilegios para **Configurar usuarios**.

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Autenticación de usuarios**. Aparecerá la página **Usuarios locales**, donde se muestran la identificación de usuario, el nombre de usuario, los privilegios del CMC y el estado de inicio de sesión de cada usuario, incluso los del usuario “raíz”. No se muestra información sobre las identificaciones de usuario disponibles para la configuración.
- 3 Haga clic en un número de identificación de usuario disponible. Aparece la página **Configuración de usuario**.
Para actualizar el contenido de la página **Usuarios**, haga clic en **Actualizar**.
Para imprimir el contenido de la página **Usuarios**, haga clic en **Imprimir**.
- 4 Seleccione la configuración general para el usuario.

Tabla 5-45. Configuración general para definir un nombre de usuario y contraseña del CMC para usuarios nuevos o ya existentes.

Propiedad	Descripción
Id. de usuario (solo lectura)	<p>Identifica a un usuario mediante uno de 16 números progresivos preconfigurados que la CLI utiliza para propósitos de secuencias de comandos. La identificación de usuario identifica al usuario particular al configurar al usuario mediante la herramienta CLI (RACADM). No puede editar la identificación del usuario.</p> <p>Si va a editar información del usuario raíz, este campo es estático. No se puede editar el nombre de usuario raíz.</p>
Activar el usuario	Activa o desactiva el acceso del usuario al CMC.
Nombre de usuario	<p>Establece o muestra el nombre de usuario exclusivo del CMC asociado con el usuario. El nombre del usuario puede contener hasta 16 caracteres. Los nombres de usuario del CMC no pueden incluir diagonales (/) ni puntos (.).</p> <p>NOTA: Si se cambia el nombre de usuario, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el siguiente inicio de sesión. Cualquier usuario que inicie sesión después de aplicar el nuevo nombre de usuario también podrá ver el cambio inmediatamente.</p>
Cambiar contraseña	<p>Permite cambiar la contraseña existente de un usuario. Establezca la nueva contraseña en el campo Contraseña nueva.</p> <p>La casilla Cambiar contraseña no podrá seleccionarse si se está configurando un nuevo usuario. Usted solo la puede seleccionar al cambiar la configuración de un usuario existente.</p>
Contraseña	Establece una contraseña nueva para un usuario existente. Para cambiar la contraseña, también debe seleccionar la casilla Cambiar contraseña . La contraseña puede contener hasta 20 caracteres, que aparecen como puntos conforme la escribe.
Confirmar la contraseña	<p>Verifica la contraseña que introdujo en el campo Contraseña nueva.</p> <p>NOTA: Los campos Contraseña nueva y Confirmar contraseña nueva solo se pueden editar cuando (1) se configura un nuevo usuario; o (2) se editan los valores de un usuario existente y la casilla Cambiar contraseña está seleccionada.</p>

- 5 Asigne el usuario al grupo de usuarios de la CMC. La Tabla 5-42 describe los privilegios de los usuarios del CMC.

Cuando seleccione un valor de privilegios de usuario en el menú desplegable **Grupo de CMC**, se mostrarán los privilegios activados (aparecerán como casillas marcadas en la lista) de acuerdo con la configuración predefinida para ese grupo.

Puede personalizar la configuración de privilegios para el usuario marcando o desmarcando las casillas. Una vez que haya seleccionado un grupo de CMC o bien haya efectuado selecciones de privilegios de usuario personalizadas, haga clic en **Aplicar cambios** para guardar la configuración.

Para actualizar el contenido de la página **Configuración de usuario**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Configuración de usuario**, haga clic en **Imprimir**.

Configuración y administración de los certificados de Microsoft Active Directory



NOTA: Para configurar los valores de Active Directory para el CMC, debe tener privilegios de **Administrador de configuración del chasis**.



NOTA: Para obtener más información acerca de la configuración de Active Directory y sobre cómo configurar Active Directory con el esquema estándar o un esquema extendido, ver “Uso del servicio de directorio del CMC” en la página 281.

Puede utilizar el servicio de Microsoft Active Directory para configurar el software para que otorgue acceso al CMC. El servicio de Active Directory le permite agregar y controlar los privilegios de los usuarios existentes del CMC.

Para acceder a la página **Menú principal de Active Directory**:

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Autenticación de usuarios** y luego en la subficha **Servicios de directorios**.
- 3 Seleccione el botón de radio del **esquema estándar** o **extendido de Microsoft Active Directory**. Aparecerán las tablas de Active Directory.

Valores comunes

Esta sección le permite configurar y ver los valores comunes de Active Directory para CMC.

Tabla 5-46. Valores comunes

Campo	Descripción
Activar Active Directory	Activa el inicio de sesión de Active Directory en CMC. Debe instalar certificados de SSL para los servidores de Active Directory que estén firmados por la misma autoridad de certificados y cargarlos en el CMC.
Activar inicio de sesión mediante tarjeta inteligente	Activa las interoperaciones de Active Directory basadas en la autenticación con Kerberos compatible con el uso de una tarjeta inteligente y un complemento de explorador proporcionado por Dell e instalado automáticamente. Para activar el uso de la tarjeta inteligente, seleccione la casilla. Para desactivar el uso de la tarjeta inteligente, deje en blanco la casilla. Si activa el uso de una tarjeta inteligente, también debe configurar la estación de trabajo cliente de Microsoft Windows para funcionar correctamente con la funcionalidad de lector de tarjeta inteligente. Esto implica instalar los controladores correctos para el lector que se utiliza y para la tarjeta inteligente que se utiliza. Los controladores de tarjeta inteligente varían según el proveedor. La tarjeta inteligente debe programarse de forma adecuada con las credenciales necesarias por medio de los servicios de inscripción de tarjeta inteligente proporcionados por el servidor de Active Directory apropiado. NOTA: Las opciones Inicio de sesión mediante tarjeta inteligente e Inicio de sesión único se excluyen mutuamente. Puede seleccionar solo una a la vez.
Activar inicio de sesión único	Permite que CMC utilice Active Directory . Para activar la opción Inicio de sesión único , seleccione la casilla. Para desactivar la opción Inicio de sesión único , deje en blanco la casilla. Si activa el Inicio de sesión único , también debe configurar las propiedades de Active Directory y seleccionar el esquema que desea utilizar. NOTA: Las opciones Inicio de sesión mediante tarjeta inteligente e Inicio de sesión único se excluyen mutuamente. Puede seleccionar solo una a la vez.

Tabla 5-46. Valores comunes (continuación)

Campo	Descripción
Activar validación de certificados de SSL	<p>Activa la validación de certificados de SSL para la conexión SSL de Active Directory del CMC. Para desactivar la validación de certificados de SSL, deje en blanco la casilla.</p> <p>PRECAUCIÓN: Si esta función se desactiva, la autenticación puede quedar expuesta al ataque de intrusos.</p> <p>El funcionamiento del explorador requiere que el acceso a CMC se realice a través de un URL HTTP que contenga una dirección de dominio completo para el CMC, esto es, http://cmc-6g2wxfl.dom.net. Una dirección IP simple para el CMC no permitirá el correcto funcionamiento del inicio de sesión único. Para admitir direcciones de dominio completo, es necesario registrar el CMC en el servicio de nombres de dominio (DNS) del servidor de Active Directory.</p> <p>Si la autenticación del explorador para el inicio de sesión único no se realiza correctamente, automáticamente se utiliza el método habitual de autenticación de explorador con nombre de usuario/contraseña local o de Active Directory. De manera similar, ante una acción de cierre de sesión después de utilizar correctamente el inicio de sesión único, se aplica el método de nombre de usuario/contraseña. El uso del inicio de sesión único está dirigido a ofrecer comodidad y no restricciones.</p> <p>NOTA: La autenticación de explorador mediante tarjeta inteligente solo se admite para exploradores Internet Explorer y clientes Microsoft Windows.</p> <p>El complemento de explorador de carga automática suministrado por Dell (control ActiveX) depende de que el sistema operativo del cliente Microsoft Windows cuente con el siguiente componente de ejecución preinstalado: Microsoft Visual C++ 2005 Redistributable Package (x86). El siguiente vínculo puede ayudar a localizar el componente: microsoft.com/downloads/details.aspx?FamilyID=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&displaylang=en. El cliente Windows necesita privilegios elevados para instalar correctamente el control ActiveX. De manera similar, la configuración del explorador requiere la capacidad de aceptar la instalación de controles ActiveX “sin firmar”.</p>

Tabla 5-46. Valores comunes (continuación)

Campo	Descripción
	La activación de la tarjeta inteligente cumple con la política de utilizar solo tarjeta inteligente para la autenticación del explorador. Todos los demás métodos de autenticación del explorador, como la autenticación con nombre de usuario/contraseña local o de Active Directory, tienen restricciones. Si se adopta la política de cumplimiento de uso de la tarjeta inteligente, es importante que el funcionamiento de la tarjeta inteligente sea completamente validado antes de desactivar los demás métodos de acceso al CMC. De lo contrario, existe la posibilidad de bloquear accidentalmente el acceso al CMC.
Nombre del dominio raíz	Especifica el nombre de dominio que Active Directory utiliza. El nombre del dominio raíz es el nombre completo con la ruta de acceso del dominio raíz para el bosque. NOTA: El nombre de dominio raíz debe ser un nombre de dominio válido que siga la convención para la asignación de nombres x.y, donde x es una cadena de 1 a 256 caracteres ASCII sin espacios en blanco entre los caracteres, en tanto y es un tipo de dominio válido, como com, edu, gov, int, mil, net u org.
Tiempo de espera de AD	Define el tiempo (expresado en segundos) que debe transcurrir para que una sesión inactiva de Active Directory se cierre automáticamente. Valores válidos: 15 a 300 segundos Valor predeterminado: 90 segundos
Especificar el servidor de AD para la búsqueda (opcional)	Cuando se selecciona, activa la llamada dirigida de la controladora de dominio y el catálogo global. Si activa esta opción, también deberá especificar las ubicaciones de la controladora de dominio y el catálogo global en la siguiente configuración. NOTA: El nombre que aparece en el certificado de CA de Active Directory no se comparará con el servidor especificado de Active Directory o el servidor de catálogo global.

Tabla 5-46. Valores comunes (continuación)

Campo	Descripción
Controlador de dominio	Especifica el servidor donde está instalado el servicio Active Directory. Esta opción solo es válida cuando la opción Especificar servidor de AD para la búsqueda (opcional) está activada.
Catálogo global	Especifica la ubicación del catálogo global en la controladora de dominio de Active Directory. El catálogo global ofrece un recurso para buscar un bosque de Active Directory. Esta opción solo es válida cuando la opción Especificar servidor de AD para la búsqueda (opcional) está activada.

Configuración del esquema estándar

Aparece la configuración del esquema estándar al seleccionar Microsoft Active Directory (Esquema estándar). Esta sección presenta los grupos de funciones con nombres, dominios y privilegios relacionados para todo grupo de funciones que ya esté configurado.

Para cambiar la configuración de un grupo de funciones, haga clic en el botón del grupo de funciones en la lista **Grupo de funciones**.



NOTA: Si hace clic en el vínculo de un grupo de funciones antes de aplicar los nuevos valores que ha introducido, perderá esos valores. Para evitar la pérdida de los nuevos valores, haga clic en **Aplicar** antes de hacer clic en el botón de un grupo de funciones.

Aparecerá la página Configurar grupo de funciones:

- Nombre de grupo: nombre que identifica el grupo de funciones en el Active Directory asociado con la tarjeta del CMC.
- Dominio del grupo: dominio en el que se ubica el grupo.
- Privilegio del grupo: nivel de privilegio para el grupo.

Haga clic en **Aplicar** para guardar los valores.

Haga clic en **Volver a la página de configuración** para regresar a la página **Servicios de directorios**.

Para actualizar el contenido de la página **Servicios de directorios**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Servicios de directorios**, haga clic en **Imprimir**.

Configuración del esquema extendido

La configuración del esquema extendido con las siguientes propiedades se muestra al seleccionar **Microsoft Active Directory (Esquema extendido)**:

- Nombre del dispositivo CMC: muestra el nombre del objeto del dispositivo de RAC creado para el CMC. El nombre del dispositivo CMC identifica de forma exclusiva la tarjeta del CMC en Active Directory. El nombre del dispositivo CMC debe ser igual al nombre común del nuevo objeto de dispositivo de RAC que se creó en la controladora de dominio. El nombre debe ser una cadena de 1 a 256 caracteres ASCII sin espacios en blanco entre los caracteres.
- Nombre de dominio del CMC: muestra el nombre DNS (cadena de caracteres) del dominio en el que reside el objeto de dispositivo de RAC de Active Directory. El dominio del CMC debe ser un nombre válido de dominio formado por x.y, donde x es una cadena de 1 a 256 caracteres ASCII sin espacios en blanco entre los caracteres, en tanto y es un tipo válido de dominio como com, edu, gov, int, mil, net u org.

Administración de certificados de Active Directory

Esta sección muestra las propiedades del certificado de Active Directory recientemente cargado en el CMC. Si carga un certificado, utilice esta información para verificar que el certificado es válido y no está vencido.



NOTA: De manera predeterminada, el CMC no tiene un certificado de servidor emitido por una autoridad de certificados para Active Directory. Usted debe cargar un certificado de servidor vigente y firmado por una autoridad de certificados.

Se muestran las siguientes propiedades del certificado:

- Número de serie: el número de serie del certificado.
- Información del titular: el titular del certificado (nombre de la persona o empresa certificada).
- Información del emisor: el emisor del certificado (nombre de la autoridad de certificados).
- Válido desde: indica la fecha de inicio del certificado.
- Válido hasta: indica la fecha de vencimiento del certificado.

Los siguientes controles le permiten cargar y descargar este certificado:

- **Cargar:** inicia el proceso de carga del certificado. Este certificado, que se obtiene de Active Directory, proporciona acceso al CMC.
- **Descargar:** inicia el proceso de descarga. El sistema le solicitará que indique una ubicación para guardar el archivo. Cuando seleccione esta opción, haga clic en **Siguiente** y aparecerá el cuadro de diálogo **Descarga de archivo**. Utilice este cuadro de diálogo para especificar una ubicación en la estación de administración o en la red compartida para el certificado de servidor.



NOTA: De manera predeterminada, el CMC no tiene un certificado de servidor emitido por una autoridad de certificados para Active Directory. Usted debe cargar un certificado de servidor vigente y firmado por una autoridad de certificados.

Archivo keytab de Kerberos

Puede cargar un archivo keytab de Kerberos generado en el servidor de Active Directory relacionado. Se puede generar el archivo keytab de Kerberos desde el servidor de Active Directory ejecutando la utilidad **ktpass.exe**. Este archivo keytab establece una relación de confianza entre el servidor Active Directory y el CMC.



NOTA: El CMC no tiene un archivo keytab de Kerberos para Active Directory. Usted debe cargar un archivo keytab de Kerberos actualmente generado. Para obtener más información, consulte "Configuración de inicio de sesión único" en la página 314.

Están permitidas las siguientes acciones:

- **Examinar:** abre el cuadro de diálogo **Examinar**, que permite seleccionar el certificado de servidor que desea cargar.
- **Cargar:** inicia el proceso de carga del certificado por medio de la ruta de acceso que haya especificado.

Configuración y administración de los servicios genéricos de protocolo ligero de acceso a directorios

Puede utilizar el servicio genérico de Protocolo ligero de acceso a directorios (LDAP) para configurar el software para que proporcione acceso al CMC. El servicio LDAP le permite agregar y controlar los privilegios de los usuarios existentes del CMC.



NOTA: Para configurar los valores de LDAP para el CMC, debe tener privilegios de **Administrador de configuración del chasis**.

Para ver y configurar LDAP:

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Autenticación de usuarios** y luego en la subficha **Servicios de directorios**. Aparecerá la página **Servicios de directorios**.
- 3 Haga clic en el botón de radio relacionado con LDAP genérico.
- 4 Configure las opciones que aparecen y haga clic en **Aplicar**.

Tabla 5-47 Enumera las opciones de configuración disponibles.

Tabla 5-47. Valores comunes

Valor	Descripción
LDAP genérico activado	Activa el servicio LDAP genérico en el CMC.
Usar nombre distintivo para buscar la pertenencia a grupos	Especifica el nombre distintivo (DN) de los grupos LDAP cuyos miembros tienen permiso para acceder al dispositivo.
Activar validación de certificados de SSL	Si esta opción está marcada, el CMC utilizará el certificado de CA para validar el certificado del servidor LDAP durante el protocolo de enlace de SSL.
DN de enlace	Especifica el nombre distintivo de un usuario que se utiliza para establecer un enlace con el servidor cuando busca el DN de usuario de inicio de sesión. Si no se indica, se utiliza un enlace anónimo.

Tabla 5-47. Valores comunes (continuación)

Valor	Descripción
Contraseña	Contraseña de enlace para utilizar junto con el DN de enlace. NOTA: La contraseña de enlace es información confidencial, por lo que debe estar protegida correctamente.
DN de base para buscar	Es el nombre de dominio de la rama del directorio donde deben iniciarse todas las búsquedas.
Atributo de inicio de sesión del usuario	Especifica el atributo que hay que buscar. Si no ha sido configurado, la opción predeterminada es utilizar uid. Se recomienda que sea único dentro del DN de base seleccionado, pues de lo contrario será necesario configurar un filtro de búsqueda para garantizar que el usuario sea único. Si el DN del usuario no puede ser identificado en forma exclusiva por la combinación de atributo y filtro de búsqueda, el inicio de sesión fallará.
Atributo de pertenencia a grupos	Especifica el atributo de LDAP que se utiliza para verificar la pertenencia a grupos. Éste deberá ser un atributo de la clase de grupos. Si se especifica, se utilizan los atributos de miembro y miembro único.
Filtro de búsqueda	Especifica un filtro de búsqueda de LDAP válido. Se utiliza cuando el atributo del usuario no puede identificar de forma exclusiva al usuario dentro del DN de base seleccionado. Si no se especifica, el valor predeterminado es (objectClass=*), que busca todos los objetos en el árbol. La longitud máxima de esta propiedad es de 1024 caracteres.
Tiempo de espera de la red (segundos)	Define el tiempo (expresado en segundos) que debe transcurrir para que una sesión inactiva de LDAP se cierre automáticamente.
Tiempo de espera de búsqueda (segundos)	Define el tiempo (expresado en segundos) que debe transcurrir para que una búsqueda se cierre automáticamente.

Selección de servidores LDAP

Puede configurar el servidor que utilizará con LDAP genérico de dos maneras. Los servidores estáticos le permiten al administrador colocar un nombre de dominio completamente expresado (FQDN) o una dirección IP en el campo. Alternativamente, puede obtenerse una lista de servidores LDAP si se buscan sus registros de SRV en los DNS. En la sección de servidores LDAP se muestran las siguientes propiedades:

- Usar servidores LDAP estáticos: al seleccionar esta opción, el servicio LDAP utiliza los servidores especificados con el número de puerto proporcionado (consulte la información a continuación).



NOTA: Debe seleccionar la opción de servidor estático o DNS.

- Dirección del servidor LDAP: permite especificar el FQDN o la dirección IP del servidor LDAP. Para especificar múltiples servidores LDAP redundantes que tienen a disposición el mismo dominio, proporcione la lista de todos los servidores separados por comas. CMC intenta conectar a cada servidor, uno por uno, hasta que logra una conexión exitosa.
- Puerto del servidor LDAP: es el puerto de LDAP a través de SSL, que de forma predeterminada será el 636 si no se configura la opción. En CMC versión 3.0 no se admite el uso de puertos que no sean SSL, ya que la contraseña no puede transportarse sin SSL.
- Usar DNS para encontrar servidores LDAP: Al seleccionar esta opción, LDAP utilizará el dominio de búsqueda y el nombre de servicio a través de DNS. Debe seleccionar la opción de servidor estático o DNS.

Se ejecutará la siguiente consulta de DNS para los registros de SRV:

```
_[Service Name] . _tcp. [Search Domain]
```

donde *<Dominio de búsqueda>* es el dominio de nivel raíz que se utiliza en la consulta y *<Nombre de servicio>* indica el nombre del servicio a 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.

Administración de la configuración de grupo de LDAP

La tabla de la sección Configuración de grupo muestra una lista de los grupos de funciones con nombres, dominios y privilegios relacionados para todo grupo de funciones que ya esté configurado.

- Para configurar un nuevo grupo de funciones, haga clic en el nombre de un grupo que no tenga nombres, dominios ni privilegios.
- Para cambiar la configuración de un grupo de funciones ya existente, haga clic en el nombre del grupo de funciones.

Al hacer clic aparecerá la página **Configurar grupo de funciones**. La ayuda para esa página está disponible mediante el vínculo **Ayuda** en la esquina superior derecha de la página.

Administración de certificados de seguridad de LDAP

Esta sección muestra las propiedades del certificado de LDAP recientemente cargado en el CMC. Si carga un certificado, utilice esta información para verificar que el certificado es válido y no está vencido.



NOTA: De manera predeterminada, el CMC no tiene un certificado de servidor emitido por una autoridad de certificados para Active Directory. Usted debe cargar un certificado de servidor vigente y firmado por una autoridad de certificados.

Se muestran las siguientes propiedades del certificado:

- Número de serie: el número de serie del certificado.
- Información del titular: el titular del certificado (nombre de la persona o empresa certificada).
- Información del emisor: el emisor del certificado (nombre de la autoridad de certificados).
- Válido desde: indica la fecha de inicio del certificado.
- Válido hasta: indica la fecha de vencimiento del certificado.

Los siguientes controles le permiten cargar y descargar este certificado:

- **Cargar:** inicia el proceso de carga del certificado. Este certificado, que se obtiene del servidor LDAP, proporciona acceso al CMC.
- **Descargar:** inicia el proceso de descarga. El sistema le solicitará que indique una ubicación para guardar el archivo. Cuando seleccione esta opción, haga clic en **Siguiente** y aparecerá el cuadro de diálogo **Descarga de archivo**. Utilice este cuadro de diálogo para especificar una ubicación en la estación de administración o en la red compartida para el certificado de servidor.

Protección de las comunicaciones del CMC con certificados SSL y digitales

Este apartado proporciona información acerca de las siguientes funciones de seguridad de datos que están incorporadas en el CMC:

- “Capa de sockets seguros (SSL)” en la página 193.
- “Solicitud de firma de certificado (CSR)” en la página 194.
- “Acceso al menú principal de SSL” en la página 195.
- “Generación de una nueva solicitud de firma de certificado” en la página 195.
- “Carga de un certificado de servidor” en la página 199.
- “Cargar clave y certificado de servidor de web” en la página 200.
- “Cómo ver un certificado de servidor” en la página 201.

Capa de sockets seguros (SSL)

El CMC incluye un servidor web que está configurado para utilizar el protocolo de seguridad SSL, que es el estándar de la industria, 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 autenticada entre los clientes y servidores a fin de evitar escuchas ilegales en una red.

La SSL permite a un sistema activado con esta característica que realice las siguientes tareas:

- Autenticarse ante un cliente activado con SSL
- Permitir que el cliente se autentique ante el servidor
- Permitir que ambos sistemas establezcan una conexión cifrada

Este proceso de cifrado proporciona una protección de datos de alto nivel. El CMC emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está normalmente disponible para los exploradores de Internet en Norteamérica.

El servidor web del CMC incluye un certificado digital SSL firmado automáticamente de Dell (identificación de servidor). Para garantizar alta seguridad en Internet, sustituya el certificado SSL de servidor de web mediante el envío de una solicitud al CMC para generar una nueva solicitud de firma de certificado (CSR).

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, esta última 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.

Acceso al menú principal de SSL



NOTA: Para configurar los valores de SSL para el CMC, debe tener 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.

Para acceder al menú principal de SSL:

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Red** y luego en la subficha **SSL**. Aparecerá la página **Menú principal de SSL**.

Utilice las opciones de la página **Menú principal de SSL** para generar una CSR para enviarla a una autoridad de certificados. La información de la solicitud de firma de certificado se almacena en el firmware del CMC.

Generación de una nueva solicitud de firma de certificado

Para garantizar la seguridad, se recomienda encarecidamente obtener y cargar un certificado de servidor seguro en el CMC. Los certificados del servidor seguro garantizan la identidad de un sistema remoto y que la información intercambiada con el sistema remoto no puede ser vista ni cambiada por otros. Sin un certificado de servidor seguro, el CMC es vulnerable a accesos por parte de usuarios no autorizados.

Tabla 5-48. Opciones del menú principal de SSL

Campo	Descripción
Generar una nueva solicitud de firma de certificado (CSR)	Seleccione esta opción y haga clic en Siguiente para abrir la página Generar una solicitud de firma de certificado (CSR) , en la que puede generar una solicitud CSR de un certificado de web segura para enviarla a una autoridad de certificados. NOTA: Cada nueva CSR sobrescribe la CSR anterior en el CMC. Para que una autoridad de certificados acepte la solicitud de firma de certificado, la solicitud en el CMC debe coincidir con el certificado recibido de la autoridad de certificados.

Tabla 5-48. Opciones del menú principal de SSL (continuación)

Campo	Descripción
Cargar certificado del servidor en base a la CSR generada	Seleccione esta opción y haga clic en Siguiente para abrir la página Carga del certificado , en la que podrá cargar un certificado existente que la empresa posea y que utilice para controlar el acceso al CMC. NOTA: El CMC solo acepta certificados codificados con X509 base 64. No acepta certificados codificados DER. Al cargar un nuevo certificado se reemplaza el certificado predeterminado que se recibió con el CMC.
Cargar clave y certificado de servidor de web	Seleccione esta opción y haga clic en Siguiente para abrir la página Carga de la clave y el certificado de servidor de web , en la que podrá cargar una clave de servidor de web y un certificado existente del servidor que la empresa posea y que utilice para controlar el acceso al CMC. NOTA: El CMC solamente acepta certificados codificados X.509 base 64. No acepta certificados codificados DER binario. Al cargar un nuevo certificado se reemplaza el certificado predeterminado que se recibió con el CMC.
Ver el certificado de servidor	Seleccione la opción y haga clic en el botón Siguiente para abrir la página Ver certificado del servidor en donde se puede ver el certificado actual del servidor.

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

Cuando se genera una CSR desde la página **Generar solicitud de firma de certificado (CSR)**, se le pide que guarde una copia 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 autenticar el certificado de servidor que reciba de la autoridad de certificados. Después de recibir el certificado del servidor de la autoridad de certificados, debe cargarlo en el CMC.



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



PRECAUCIÓN: Cuando se genera una nueva CSR, ésta sobrescribe la CSR anterior que esté en el CMC. Si se sobrescribe una CSR pendiente antes de que la autoridad de certificados otorgue el certificado de servidor correspondiente, el CMC no aceptará el certificado de servidor porque la información que utilizar para autenticar el certificado se ha perdido. Tome las precauciones necesarias al generar una CSR a fin de evitar sobrescribir las CSR pendientes.

Para generar una CSR:

- 1 Desde la página **Menú principal de SSL**, seleccione **Generar una nueva solicitud de firma de certificado (CSR)** y luego haga clic en **Siguiente**. Aparecerá la página **Generar solicitud de firma de certificado (CSR)**.
- 2 Escriba un valor para cada atributo de la CSR.
- 3 Haga clic en **Generate** (Generar). Aparecerá un cuadro de diálogo **Descarga de archivo**.
- 4 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.) Más adelante, enviará este archivo a una autoridad de certificados.

Tabla 5-49. Opciones de la página Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	<p>El nombre exacto que se está certificando (generalmente el nombre de dominio del servidor de web, por ejemplo, www.empresa_xyz.com/).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9); guiones, guiones bajos y puntos.</p> <p>Valores no válidos: caracteres no alfanuméricos distintos a los que se indicaron anteriormente (por ejemplo, @ # \$ % & *, entre otros); caracteres que se utilizan principalmente en idiomas distintos al inglés, por ejemplo, ß, å, é, ü.</p>
Nombre de la organización	<p>El nombre asociado con su organización (por ejemplo: Empresa XYZ).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9); guiones, guiones bajos, puntos y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>
Unidad organizacional	<p>El nombre relacionado con la unidad organizacional, como un departamento (por ejemplo: Grupo de servidores empresariales).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9); guiones, guiones bajos, puntos y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>
Localidad	<p>La ciudad o ubicación de la organización (ejemplos: Atlanta, Hong Kong).</p> <p>Valores válidos: caracteres alfanuméricos (A-Z, a-z, 0-9) y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>

Tabla 5-49. Opciones de la página Generar solicitud de firma de certificado (CSR)

Campo	Descripción
Estado	<p>El estado, provincia o territorio donde se encuentra la entidad que solicita la certificación (ejemplos: Texas, Nueva Gales del Sur, Andhra Pradesh).</p> <p>NOTA: No utilice abreviaturas.</p> <p>Valores válidos: caracteres alfanuméricos (letras mayúsculas y minúsculas, 0-9) y espacios.</p> <p>Valores no válidos: caracteres no alfanuméricos no indicados anteriormente (por ejemplo, @ # \$ % & *, entre otros).</p>
País	<p>El país donde se encuentra la organización que solicita la certificación.</p>
Correo electrónico	<p>Dirección de correo electrónico de su empresa. Puede escribir cualquier dirección de correo electrónico que desee tener asociada con la CSR. La dirección de correo electrónico debe ser válida y contener el signo arroba (@) (por ejemplo: nombre@empresaxyz.com).</p> <p>NOTA: Esta dirección de correo electrónico es un campo opcional.</p>

Carga de un certificado de servidor

Para cargar un certificado del servidor:

- 1** En la página **Menú principal de SSL**, seleccione **Cargar certificado del servidor basado en CSR generada** y luego haga clic en **Siguiente**. Aparecerá la página **Carga del certificado**.
- 2** Escriba la ruta de acceso del archivo en el campo de texto o haga clic en **Examinar** para seleccionar el archivo.
- 3** Haga clic en **Aplicar**. Si el certificado no es válido, aparecerá un mensaje de error.



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

Para actualizar el contenido de la página **Carga del certificado**, haga clic en **Actualizar**.

Para imprimir el contenido de la página **Carga del certificado**, haga clic en **Imprimir**.

Cargar clave y certificado de servidor de web

Para cargar una clave y certificado de servidor de web

- 1 Seleccione la opción **Cargar clave y certificado de servidor de web** y haga clic en **Siguiente**.
- 2 Ingrese el archivo de clave privada por medio del menú Examinar.
- 3 Ingrese el archivo de certificado por medio del menú Examinar.
- 4 Después de cargar los dos archivos, haga clic en **Aplicar**. Si la clave y el certificado de servidor de web no coinciden, aparecerá un mensaje de error.



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



NOTA: Para cargar una clave y certificado de servidor de servidor de web debe tener privilegios de **Administrador de configuración del chasis**.



NOTA: Una vez que el certificado se ha cargado correctamente, CMC se reinicia y deja de estar disponible temporalmente. Para evitar que se desconecte a 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 hay sesiones activas.

Cómo ver un certificado de servidor

Desde la página **Menú principal de SSL**, seleccione **Ver certificado del servidor** y luego haga clic en **Siguiente**. Aparecerá la página **Ver certificado del servidor**.

La Tabla 5-50 describe los campos asociados con las descripciones que aparecen en la ventana **Certificado**.

Tabla 5-50. Información de certificados

Campo	Descripción
Serie	El número de serie del certificado.
Titular	Los atributos del certificado introducidos por el titular.
Emisor	Los atributos del certificado generados por el emisor.
notBefore	Fecha de emisión del certificado.
notAfter	Fecha de vencimiento del certificado.

Para actualizar el contenido de la página **Ver certificado del servidor** haga clic en **Actualizar**.

Para imprimir el contenido de la página **Ver certificado del servidor**, haga clic en **Imprimir**.

Administración de sesiones

La página **Sesiones** muestra todas las instancias actuales de las conexiones al chasis y le permite terminar cualquier sesión activa.



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

Para administrar o terminar una sesión:


- 1 Inicie sesión en el CMC a través de la web.
- 2 Haga clic en la ficha **Red** y luego en la subficha **Sesiones**.
- 3 En la página **Sesiones**, ubique la sesión que desea terminar y haga clic en el botón correspondiente. Tabla 5-51 muestra las propiedades de la sesión.


Tabla 5-51. Propiedades de la sesión


Propiedad	Descripción
Identificación de sesión	Muestra el número de identificación generado progresivamente para cada inicio de sesión.
Nombre de usuario	Muestra el nombre de inicio de sesión del usuario (usuario local o usuario de Active Directory). Algunos ejemplos de nombres de usuario de Active Directory son <i>nombre@dominio.com</i> , <i>dominio.com/nombre</i> , <i>dominio.com\nombre</i> .
Dirección IP	Muestra la dirección IP del usuario.
Tipo de sesión	Describe el tipo de sesión: Telnet, serie, SSH, RACADM remoto, SMASH CLP, WSMAN o interfaz gráfica de usuario.
Terminar	Le permite terminar cualquiera de las sesiones de la lista, excepto la suya. Para terminar la sesión relacionada, haga clic en el botón. Esta columna solo aparecerá si usted tiene privilegios de Administrador de configuración del chasis .

Configuración de servicios

El CMC incluye un servidor de web que está configurado para utilizar el protocolo de seguridad SSL estándar de la industria para aceptar y transferir datos cifrados de y para clientes en Internet. El servidor de web incluye un certificado digital SSL de Dell autofirmado (identificación del servidor) y es responsable de aceptar y responder solicitudes de HTTP seguras de clientes. La interfaz web y la herramienta de CLI remota requieren este servicio para comunicarse con el CMC.

 **NOTA:** La herramienta de CLI remota (RACADM) y la interfaz web utilizan el servidor de web. Si el servidor de web no está activo, RACADM remoto y la interfaz web no funcionarán.

 **NOTA:** En caso de un restablecimiento del servidor de web, espere al menos un minuto para que los servicios estén disponibles de nuevo. Un restablecimiento del servidor de web generalmente sucede como resultado de cualquiera de los siguientes sucesos: la configuración de la red o las propiedades de seguridad de la red se han cambiado mediante la interfaz de usuario web del CMC o RACADM; la configuración del puerto del servidor de web se ha cambiado mediante la interfaz de usuario web o RACADM; el CMC se ha restablecido; se cargó un certificado nuevo del servidor SSL.

 **NOTA:** Para modificar la configuración de los servicios, debe tener privilegios de **Administrador de configuración del chasis**.

Para configurar los servicios del CMC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en la ficha **Red**.
- 3 Haga clic en la subficha **Servicios**. Aparecerá la página **Servicios**.
- 4 Configure los servicios siguientes según sea necesario:
 - Consola serie del CMC (Tabla 5-52)
 - Servidor de web (Tabla 5-53)
 - SSH (Tabla 5-54)
 - Telnet (Tabla 5-55)
 - RACADM remoto (Tabla 5-56)
 - SNMP (Tabla 5-57)
 - Syslog remoto (Tabla 5-58)
- 5 Haga clic en **Aplicar** y actualice todos los intervalos de tiempo de espera predeterminados y los límites máximos de tiempo de espera.

Tabla 5-52. Configuración de la consola serie del CMC

Valor	Descripción
Activado	Activa la interfaz de la consola Telnet del CMC. Valor predeterminado: sin seleccionar (desactivada).
Redirección activada	Activa la redirección de la consola serie/de texto al servidor a través del cliente serie, Telnet o SSH desde el CMC. El CMC se conecta con el iDRAC, que se conecta internamente con el puerto COM2 del servidor. Opciones de configuración: seleccionado (activado), sin seleccionar (desactivado) Valor predeterminado: seleccionado (activado)

Tabla 5-52. Configuración de la consola serie del CMC (continuación)

Valor	Descripción
Tiempo de espera en inactividad	<p>Muestra el número de segundos antes de que una sesión serie inactiva se desconecte automáticamente. Un cambio en el valor Tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual.</p> <p>Rango de tiempo de espera: 0 ó 60 hasta 10800 segundos. Para desactivar la función de tiempo de espera, introduzca 0.</p> <p>Valor predeterminado: 1800 segundos.</p>
Velocidad en baudios	<p>Muestra la velocidad de los datos en el puerto serie externo del CMC.</p> <p>Opciones de configuración: 9600, 19200, 28800, 38400, 57600 y 115200 bps.</p> <p>Valor predeterminado: 115200 bps.</p>
Autenticación desactivada	<p>Activa la autenticación del inicio de sesión de la consola serie del CMC.</p> <p>Valor predeterminado: sin seleccionar (desactivada).</p>

Tabla 5-52. Configuración de la consola serie del CMC (continuación)

Valor	Descripción
Tecla Esc	<p>Permite especificar la combinación de la tecla Esc que termina la redirección de la consola serie/de texto cuando se utiliza el comando connect o racadm connect.</p> <p>Valor predeterminado: ^\ Mantenga presionada la tecla <Ctrl> y presione la tecla de barra diagonal invertida (\)</p> <p>NOTA: El carácter de intercalación ^ representa la tecla <Ctrl>.</p> <p>Opciones de configuración:</p> <ul style="list-style-type: none">• Valor decimal (ejemplo: 95)• Valor hexadecimal (por ejemplo: 0x12)• Valor octal (ejemplo: 007)• Valor ASCII (ejemplo: ^ a) <p>Los valores ASCII se pueden representar utilizando los siguientes códigos de la tecla Esc:</p> <ul style="list-style-type: none">• Esc seguido de un carácter alfabético (a-z, A-Z)• Esc seguido de los siguientes caracteres especiales: [] \ ^ _• Longitud máxima permitida: 4
Tamaño del búfer de historial	<p>Muestra el tamaño máximo del búfer del historial serie, que contiene los últimos caracteres escritos en la consola serie.</p> <p>Valor predeterminado: 8192 caracteres.</p>
Comando de inicio de sesión	<p>Especifica el comando serie que se ejecuta automáticamente cuando un usuario se conecta a la interfaz de la consola serie del CMC.</p> <p>Ejemplo: connect server-1</p> <p>Valor predeterminado: [Nulo]</p>

Tabla 5-53. Configuración del servidor Web

Valor	Descripción
Activado	Activa los servicios de servidor de web (acceso mediante RACADM remoto y la interfaz web) para el CMC. Valor predeterminado: seleccionado (activado).
N.º máx. de sesiones	Muestra el número máximo de sesiones simultáneas de la interfaz web del usuario permitidas para el chasis. Un cambio en la propiedad N.º máx. de sesiones tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluso la suya). La propiedad N.º máx. de sesiones para el servidor de web no afecta a RACADM remoto. Rango permitido: 1 a 4 Valor predeterminado: 4 NOTA: Si cambia la propiedad N.º máx. de sesiones a un valor menor que el número de sesiones activas actuales y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.
Tiempo de espera en inactividad	Muestra el número de segundos antes de que una sesión de interfaz web del usuario inactiva se desconecte automáticamente. Un cambio en el valor Tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual. Rango de tiempo de espera: 60 a 10800 segundos. Valor predeterminado: 1800 segundos.

Tabla 5-53. Configuración del servidor Web (continuación)

Valor	Descripción
Número de puerto de HTTP	<p>Muestra el puerto predeterminado utilizado por el CMC en espera de una conexión de servidor.</p> <p>NOTA: Cuando se proporciona una dirección HTTP en el explorador, el servidor de web se redirige automáticamente y utiliza HTTPS.</p> <p>Si se ha cambiado el número predeterminado del puerto HTTPS predeterminado (80), debe incluir el número de puerto en la dirección introducida en el campo de dirección del explorador, como se muestra:</p> <p style="padding-left: 40px;"><code>http://<Dirección IP >:<número de puerto ></code></p> <p>donde <i>Dirección IP</i> es la dirección IP del chasis y <i>número de puerto</i> es el número de puerto HTTP distinto al predeterminado: 80.</p> <p>Rango de configuración:10 a 65535</p> <p>Valor predeterminado: 80</p>
Número de puerto HTTPS	<p>Muestra el puerto predeterminado utilizado por el CMC en espera de una conexión segura de servidor.</p> <p>Si el número del puerto HTTPS predeterminado (443) se ha cambiado, debe incluir el número de puerto en la dirección introducida en campo de dirección del explorador, como se muestra:</p> <p style="padding-left: 40px;"><code>https://<Dirección IP >:<número de puerto></code></p> <p>donde <i><Dirección IP ></i> es la dirección IP del chasis y <i>número de puerto</i> es el número de puerto HTTPS distinto al valor predeterminado de 443.</p> <p>Rango de configuración:10 a 65535</p> <p>Valor predeterminado: 443</p>

Tabla 5-54. Configuración de SSH

Valor	Descripción
Activado	Activa el SSH en el CMC. Valor predeterminado: seleccionado (activado).
N.º máx. de sesiones	El número máximo de sesiones simultáneas de SSH permitidas para el chasis. Un cambio en esta propiedad tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluso la suya). Rango configurable: 1 a 4 Valor predeterminado: 4 NOTA: Si cambia la propiedad N.º máx. de sesiones a un valor menor que el número actual de Sesiones activas y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.
Tiempo de espera en inactividad	Muestra el número de segundos antes de que una sesión SSH inactiva se desconecte automáticamente. Un cambio en el valor Tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual. Rango de tiempo de espera: 0 ó 60 – 10800 segundos. Para desactivar la función de tiempo de espera, introduzca 0. Valor predeterminado: 1800 segundos.
Número de puerto	El puerto utilizado por el CMC que espera una conexión de servidor. Rango de configuración: 10 a 65535 Valor predeterminado: 22

Tabla 5-55. Configuración de Telnet

Valor	Descripción
Activado	Activa la interfaz de la consola Telnet del CMC. Valor predeterminado: sin seleccionar (desactivada).
N.º máx. de sesiones	Muestra el número máximo de sesiones de Telnet simultáneas permitidas para el chasis. Un cambio en esta propiedad tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluso la suya). Rango permitido: 1 a 4 Valor predeterminado: 4 NOTA: Si cambia la propiedad N.º máx. de sesiones a un valor menor que el número de Sesiones activas actuales y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.
Tiempo de espera en inactividad	Muestra el número de segundos antes de que una sesión de Telnet inactiva se desconecte automáticamente. Un cambio en el valor del tiempo de espera tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual. Rango de tiempo de espera: 0 ó 60 – 10800 segundos. Para desactivar la función de tiempo de espera, introduzca 0. Valor predeterminado: 1800 segundos.
Número de puerto	Muestra el puerto predeterminado utilizado por el CMC en espera de una conexión de servidor. Valor predeterminado: 23

Tabla 5-56. Configuración de RACADM remota

Valor	Descripción
Activado	Activa el acceso de la utilidad RACADM remoto al CMC. Valor predeterminado: seleccionado (activado).
N.º máx. de sesiones	Muestra el número máximo de sesiones de RACADM simultáneas permitidas para el chasis. Un cambio en esta propiedad tiene efecto en el siguiente inicio de sesión; no afecta las sesiones activas actuales (incluso la suya). Rango permitido: 1 a 4 Valor predeterminado: 4 NOTA: Si cambia la propiedad N.º máx. de sesiones a un valor menor que el número de Sesiones activas actuales y luego se desconecta, no podrá volver a conectarse hasta que las otras sesiones hayan terminado o expirado.
Tiempo de espera en inactividad	Muestra el número de segundos antes de que una sesión de racadm inactiva se desconecte automáticamente. Un cambio en el valor Tiempo de espera en inactividad tiene efecto en el siguiente inicio de sesión; no afecta la sesión actual. Para desactivar la función Tiempo de espera en inactividad, introduzca 0. Rango de tiempo de espera: 0 ó 10 hasta 1920 segundos. Para desactivar la función de tiempo de espera, introduzca 0. Valor predeterminado: 30 segundos.

Tabla 5-57. Configuración de SNMP

Valor	Descripción
Activado	Activa SNMP en el CMC. Valores válidos: seleccionado (activado), sin seleccionar (desactivado) Valor predeterminado: sin seleccionar (desactivado)
Nombre de comunidad	Muestra la cadena de comunidad utilizada para obtener datos del daemon SNMP del CMC.

Tabla 5-58. Configuración de Syslog remoto

Valor	Descripción
Activado	Activa la transmisión y la captura remota de las anotaciones del registro de CMC y el registro de hardware de los servidores especificados. Valores válidos: seleccionado (activado), sin seleccionar (desactivado) Valor predeterminado: sin seleccionar (desactivado)
Servidor Syslog 1	Es el primero de los tres servidores en albergar una copia de las anotaciones de los registros de CMC y hardware. Se especifica con un nombre de host, una dirección IPv6 o una dirección IPv4.
Servidor Syslog 2	Es el segundo de los tres servidores en albergar una copia de las anotaciones de los registros de CMC y hardware. Se especifica con un nombre de host, una dirección IPv6 o una dirección IPv4.
Servidor Syslog 3	Es el tercero de los tres servidores en albergar una copia de las anotaciones de los registros de CMC y hardware. Se especifica con un nombre de host, una dirección IPv6 o una dirección IPv4.
Número de puerto de Syslog	Especifica el número del puerto en el servidor remoto que recibe una copia de las anotaciones de los registros de CMC y hardware. Se utiliza el mismo número de puerto para los tres servidores. Un número de puerto de syslog válido se encuentra en el rango de 10 a 65535. Valor predeterminado: 514

Configuración del presupuesto de alimentación

El CMC le permite administrar la alimentación para el chasis. El servicio de administración de alimentación optimiza el consumo de energía y reasigna la alimentación eléctrica a los distintos módulos en función de la demanda.

Para obtener instrucciones acerca de cómo configurar la alimentación mediante el CMC, ver “Configuración y administración de la alimentación” en la página 356.

Para obtener más información acerca del servicio de administración de la alimentación del CMC, ver “Administración de la alimentación” en la página 333.

Administración de actualizaciones de firmware

En esta sección se explica cómo actualizar el firmware de los componentes del servidor y el chasis con la interfaz gráfica de usuario y la utilidad RACADM.

Los componente siguientes se pueden actualizar con RACADM o la interfaz gráfica de usuario. En la interfaz gráfica de usuario puede realizar la actualización a través de las páginas **Descripción general del chasis**→ **Actualizar** o **Controlador del chasis**→ **Actualizar**:

- CMC: activo y en espera
- iKVM
- iDRAC: el firmware de los iDRAC anteriores a iDRAC6 debe actualizarse con la interfaz de recuperación. El firmware del iDRAC6 también se puede actualizar con la interfaz de recuperación, pero esta ha caído en desuso en el iDRAC6 y las versiones posteriores.
- Servicios de infraestructura del módulo de E/S

En la página **Descripción general de servidores**→ **Actualizar** de la interfaz gráfica de usuario, puede actualizar los siguientes componentes de servidor.

- iDRAC
- BIOS
- Unified Server Configurator (Configurador de servidor unificado)
- Diagnósticos de 32 bits
- OS-Drivers Pack
- Controladores de interfaz de red
- Controladores RAID


Las actualizaciones del firmware de los componentes del servidor se realizan mediante el servidor Lifecycle Controller disponible en el iDRAC. Lifecycle Controller admite imágenes de firmware en el formato Dell Update Package (DUP). La configuración predeterminada del CMC tiene un límite de tamaño de 48MB del DUP. El DPU del componente OS-Driver Pack supera este límite y debe actualizarse por separado con la función Almacenamiento extendido. Para obtener más información, ver “Actualización del firmware de los componentes de servidor mediante Lifecycle Controller” en la página 222.

Cuando se actualiza el firmware, se recomienda seguir un proceso que puede evitar una pérdida del servicio si la actualización falla. Si desea conocer las pautas a seguir, consulte la sección “Instalación o actualización del firmware de la CMC” en la página 56.

Cómo ver las versiones actuales del firmware

La página Actualización muestra la versión actual de todos los componentes que se pueden actualizar en el chasis. Esto puede incluir el firmware del iKVM, el firmware del CMC activo, (si corresponde), el firmware del CMC en espera, el firmware del iDRAC y el firmware de los dispositivos de infraestructura del módulo de E/S. Para obtener más información, consulte “Actualización del firmware de los dispositivos de infraestructura del módulo de E/S” en la página 218.

Para ver los componentes del chasis que se pueden actualizar:

- 1 Inicie sesión en la interfaz web. Para obtener más información, consulte “Acceso a la interfaz web del CMC” en la página 115.
- 2 Haga clic en **Descripción general del chasis** en el árbol del sistema.
 **NOTA:** Como alternativa, haga clic en **Controlador del chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Actualizar**. Aparecerá la página **Actualización del firmware**.

Para visualizar los componentes del servidor que se pueden actualizar:

- 1 Inicie sesión en la interfaz web. Para obtener más información, consulte “Acceso a la interfaz web del CMC” en la página 115.
- 2 Haga clic en **Descripción general de servidores** en el árbol del sistema.
- 3 Haga clic en la ficha **Actualizar**. Aparecerá la página **Actualización de componentes de servidor**.

Para abrir una página de actualización para los dispositivos seleccionados:

- 1 Haga clic en el nombre del dispositivo o seleccione la opción **Seleccionar/Deseleccionar todo**.
- 2 Haga clic en **Aplicar actualización**.

Aparecerá una página de actualización para los dispositivos seleccionados.

Si el chasis contiene un servidor de una generación anterior cuyo iDRAC está en modo de recuperación o si el CMC detecta que un iDRAC tiene el firmware dañado, el iDRAC de generación anterior también aparece en la página Actualización del firmware. Para ver los pasos para recuperar el firmware del iDRAC mediante el CMC, ver “Recuperación del firmware del iDRAC por medio del CMC” en la página 220.

Actualización del firmware



NOTA: Para actualizar el firmware del CMC, debe tener privilegios de Administrador de configuración del chasis.



NOTA: La actualización del firmware conserva la configuración actual del CMC y del iKVM.



NOTA: Si se utiliza una sesión de interfaz de usuario web para actualizar el firmware de los componentes del sistema, debe establecerse un valor suficientemente elevado de **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**, ver “Configuración de servicios” en la página 202.

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

Los pasos necesarios para actualizar firmware de dispositivos son:

- 1 Seleccione los dispositivos a actualizar.
- 2 Haga clic en el botón **Aplicar** debajo del grupo.
- 3 Haga clic en **Examinar** para seleccionar la imagen de firmware.
- 4 Haga clic en **Iniciar actualización del firmware** para iniciar el proceso de actualización. Aparecerá un mensaje que dice **Transfiriendo imagen de archivo**, seguido de una página de estado del progreso.



NOTA: Asegúrese de tener la versión más reciente del firmware. Puede descargar la versión más reciente del archivo de imagen del firmware en el sitio web del servicio de asistencia Dell Support en support.dell.com.


Actualización de firmware del CMC





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



NOTA: El CMC activo se restablecerá y no estará disponible temporalmente después de que el firmware se haya cargado correctamente. 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 solo al CMC activo, después de que se haya 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 en espera.


 **NOTA:** Para evitar que se desconecte a otros usuarios durante el restablecimiento, notifique a los usuarios autorizados que puedan tratar de iniciar sesión en el CMC y consulte la página **Sesiones** para comprobar si hay sesiones activas. Para abrir la página **Sesiones**, seleccione **Chasis** en el árbol, haga clic en la ficha **Red** y luego haga clic en la subficha **Sesiones**. La ayuda para esa página está disponible mediante el vínculo **Ayuda** en la esquina superior derecha de la página.

 **NOTA:** Al transferir archivos al CMC y desde el mismo, 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, ver “Habilitación de animaciones en Internet Explorer” en la página 45.

 **NOTA:** Si experimenta problemas al descargar archivos desde el CMC utilizando Internet Explorer, active la opción **No guardar páginas cifradas en el disco**. Consulte la sección “Descarga de archivos desde el CMC con Internet Explorer” en la página 45 para obtener instrucciones.

Actualizar el firmware del CMC

- 1 En la página **Actualización del firmware**, seleccione los CMC que desee actualizar marcando la casilla **Actualizar destinos** de los CMC. Ambos CMC pueden actualizarse al mismo tiempo.
- 2 Haga clic en el botón **Aplicar actualización del CMC** debajo de la lista de componentes de CMC.

 **NOTA:** El nombre predeterminado de la imagen del firmware del CMC es **firmimg.cmc**. El firmware del CMC debe actualizarse primero, antes de actualizar el firmware del dispositivo de infraestructura del módulo de E/S.

- 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.

4 Haga clic en **Iniciar actualización del firmware**. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar mucho en función de la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Instrucciones adicionales que hay que seguir:

- No utilice el botón **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 estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos.



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

5 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 del firmware, la sesión del explorador y la conexión con el CMC se perderán temporalmente debido a que el CMC activo se desconecta. Debe iniciar sesión después de unos minutos, cuando el CMC activo se haya reiniciado. Después de que el CMC se haya restablecido, el nuevo firmware aparecerá en la página **Actualización del firmware**.



NOTA: Después de actualizar el firmware, borre la caché del explorador de web. Consulte la ayuda en línea de su explorador de web para obtener instrucciones acerca de cómo borrar la caché del explorador.

Actualización del firmware de iKVM



NOTA: Una vez que se ha cargado el firmware correctamente, iKVM se reinicia y deja de estar disponible temporalmente.

- 1 Vuelva a iniciar sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Actualizar**. Aparecerá la página **Actualización del firmware**.

- 4 Seleccione el iKVM para actualizar la casilla **Actualizar destinos** para ese iKVM.
- 5 Haga clic en el botón **Aplicar actualización del iKVM** debajo de la lista de componentes de iKVM.
- 6 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.



NOTA: El nombre predeterminado de la imagen del firmware de iKVM es `kvm.bin`, aunque el usuario puede cambiarlo para evitar confusiones con imágenes anteriores.

- 7 Haga clic en **Iniciar actualización del firmware**.
- 8 Haga clic en **Sí** para continuar. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar mucho en función de la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Instrucciones adicionales que hay que seguir:
 - No utilice el botón **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 estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos.



NOTA: La actualización del iKVM puede requerir de hasta dos minutos.

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

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

Al realizar esta actualización, se actualiza el firmware para un componente del dispositivo del módulo de E/S, pero no el firmware del dispositivo mismo; el componente es el circuito de interfaz entre el dispositivo del 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 gráfica de usuario de web de CMC solo si la revisión actual en el componente y la imagen del componente en el CMC no coinciden. Para actualizar el firmware de los dispositivos de infraestructura del módulo de E/S:

- 1 Vuelva a iniciar sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Actualizar**. Aparecerá la página **Actualización del firmware**.
- 4 Seleccione el dispositivo del módulo de E/S que desea actualizar seleccionando la casilla **Actualizar destinos** del dispositivo del módulo de E/S.
- 5 Haga clic en el botón **Aplicar actualización del módulo de E/S** debajo de la lista de componentes de módulo de E/S.



NOTA: El campo **Imagen del firmware** no se muestra para los destinos de dispositivo de infraestructura del módulo de E/S (IOMINF) porque la imagen requerida reside en el CMC. El firmware del CMC debe actualizarse primero, antes de actualizar el firmware de la infraestructura del módulo de E/S.

El CMC autoriza las actualizaciones del dispositivo de infraestructura del módulo de E/S cuando detecta que el firmware del mismo no está actualizado con la imagen que se encuentra en el sistema de archivos del CMC. Si el firmware del dispositivo de infraestructura del módulo de E/S está actualizado, el CMC impedirá su actualización. Los dispositivos de infraestructura del módulo de E/S actualizados aparecen como dispositivos actualizables.

6 Haga clic en **Iniciar actualización del firmware**. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar mucho en función de la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el cronómetro de actualización del firmware. Instrucciones adicionales que hay que seguir:

- No utilice el botón **Actualizar** ni visite otra página durante la transferencia de archivos.
- El estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos.



NOTA: No aparecerá ningún cronómetro de transferencia cuando se actualiza el firmware de dispositivo de infraestructura del módulo de E/S. El proceso de actualización puede causar una breve pérdida de la conectividad en el dispositivo del módulo de E/S porque el dispositivo se reiniciará cuando se complete la actualización. Una vez que se completa la actualización, se muestra el nuevo firmware y el sistema actualizado deja de aparecer en la página **Actualización del firmware**.

Actualización del firmware del iDRAC del servidor




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



NOTA: El firmware del iDRAC debe ser de la versión 1.4 o superior para los servidores con iDRAC, o 2.0 o superior para los servidores con iDRAC6 Enterprise. Si va a actualizar el firmware del iDRAC a la versión 3.0 o una versión superior desde una versión anterior a 2.3, antes debe actualizarlo a la versión 2.3 antes de actualizarlo a la versión 3.0 o superior.

- 1** Vuelva a iniciar sesión en la interfaz web del CMC.
- 2** Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3** Haga clic en la ficha **Actualizar**. Aparecerá la página **Actualización del firmware**.
- 4** Seleccione los iDRAC que desee actualizar seleccionando la casilla **Actualizar destinos** de dichos dispositivos.

- 5 Haga clic en el botón **Aplicar actualización del iDRAC** debajo de la lista de componentes de iDRAC.
- 6 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.
- 7 Haga clic en **Iniciar actualización del firmware**. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar mucho en función de la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el temporizador de actualización del firmware. Instrucciones adicionales que hay que seguir:
 - No utilice el botón **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 estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos.

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

Recuperación del firmware del iDRAC por medio del 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 comando SM-CLP o los paquetes de actualización específicos del sistema operativo descargados desde support.dell.com. Consulte la *Guía del usuario del firmware del iDRAC* para ver instrucciones acerca de cómo actualizar el firmware del iDRAC.

Las generaciones tempranas de servidores pueden restablecer 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**.

Actualizar el firmware del CMC.

- 1 Descargue el firmware del iDRAC más reciente en el equipo de administración de la dirección support.dell.com.
- 2 Inicie sesión en la interfaz web (ver “Acceso a la interfaz web del CMC” en la página 115).
- 3 Haga clic en **Descripción general del chasis** en el árbol del sistema.
- 4 Haga clic en la ficha **Actualizar**. Aparecerá la página **Actualización del firmware**.
- 5 Seleccione los iDRAC del mismo modelo que desee actualizar seleccionando la casilla **Actualizar destinos** de dichos dispositivos.
- 6 Haga clic en el botón **Aplicar actualización del iDRAC** debajo de la lista de componentes de iDRAC.
- 7 Haga clic en **Examinar**, vaya a la imagen del firmware del iDRAC que descargó y haga clic en **Abrir**.



NOTA: El nombre predeterminado de la imagen del firmware del iDRAC es **firmimg.imc**. El firmware del CMC debe actualizarse primero, antes de actualizar el firmware del dispositivo de infraestructura del módulo de E/S.

- 8 Haga clic en **Iniciar actualización del firmware**. Instrucciones adicionales que hay que seguir:
 - No utilice el botón **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 estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos.



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

Actualización del firmware de los componentes de servidor mediante Lifecycle Controller

Lifecycle Controller es un servicio que está disponible en cada servidor y lo proporciona iDRAC. La página **Actualización de componentes de servidor** le permite administrar el firmware de los componentes y dispositivos en los servidores por medio del servicio Lifecycle Controller. Lifecycle Controller utiliza un algoritmo de optimización para actualizar el firmware que reduce eficazmente el número de reinicios.

Antes de utilizar la función de actualización basada en Lifecycle Controller, deben actualizarse las versiones del firmware del servidor.



NOTA: Actualice el firmware del CMC antes de actualizar los módulos de firmware de los componentes de servidor.

Los módulos de firmware de los componentes de servidor deben actualizarse en este orden:

- BIOS
- Controlador del ciclo de vida
- iDRAC

Consulte la sección “Recommended Module Firmware Versions” (Versiones recomendadas de firmware del módulo) del archivo Léame del CMC en el sitio support.dell.com/manuals. Lifecycle Controller proporciona soporte de actualización de módulos para servidores iDRAC6 y posteriores. Para actualizar el firmware del iDRAC con Lifecycle Controller, debe tener la versión de firmware 2.3 o superior.

Si actualiza el firmware manualmente con DUP, debe seguir este orden:

- BIOS
- Lifecycle Controller
- iDRAC: si va a actualizar el firmware del iDRAC a la versión 3.0 o una versión superior desde una versión anterior a 2.3, antes debe actualizarlo a la versión 3.0 o superior.

Cómo activar Lifecycle Controller

Si el servidor no es compatible con el servicio Lifecycle Controller, la sección de **Inventario de firmware** aparece como **No compatible**.

El servicio Lifecycle Controller pueden estar desactivado en el servidor y la sección **Inventario de firmware** aparece como **Lifecycle Controller** puede no estar activado.

Para activar el servicio Lifecycle Controller en la última generación de servidores, actualice los servidores existentes por medio de instalar el firmware de Unified Server Configurator (USC) y de iDRAC. Es posible que esta actualización no se pueda realizar en servidores de la generación anterior.

Normalmente, el firmware de USC se instala con el paquete apropiado que se tiene que ejecutar en el servidor OS. Un paquete de reparación o instalación especial con la extensión de archivo **.usc** está disponible en la interfaz web nativa del explorador iDRAC. Este paquete le permite instalar el firmware USC por medio de los servicios habituales de actualización de firmware.

Para obtener más información, consulte la *Dell Lifecycle Controller USC/USC-LCE User's Guide* (Guía del usuario de Dell Lifecycle Controller para USC/USC-LCE).

El servicio Lifecycle Controller se puede activar durante el proceso de reinicio 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 s**, pulse **<Ctrl+E>**. Después, en la pantalla Configuración, active **Servicios del sistema**.

Para cancelar todos los trabajos programados que están pendientes y quitarlos de la cola, seleccione **Cancelar servicios del sistema**.

En la página **Actualización de componentes de servidor**, puede actualizar varios componentes del firmware del sistema. Para utilizar las funciones y acciones de esta página, debe 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 componentes y dispositivos en el servidor. No puede seleccionar ningún componente o dispositivo de ningún tipo de operación de Lifecycle Controller en el servidor.

Para obtener más información sobre Lifecycle Controller y componentes de servidor, y administración de firmware de dispositivos, ver:

- Información general de los Servicios remotos de Lifecycle Controller.
- delltechcenter.com/page/Lifecycle+Controller.

Mecanismos de filtrado

Se recupera a la vez información de todos los componentes y dispositivos en todos los servidores. Para administrar esta gran cantidad de información, Lifecycle Controller proporciona varios mecanismos de filtrado. Estos filtros le permiten:

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



NOTA: La función de filtro automático es importante al utilizar el Dell Update Package (DUP). La actualización de un DUP puede estar basada en el tipo o modelo del componente o dispositivo. El comportamiento de los filtros automáticos está diseñado para minimizar las decisiones siguientes después de haber realizado una selección inicial.

Ejemplos

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

- Si está seleccionado el filtro BIOS, solo aparece el inventario de BIOS para todos los servidores. Si el conjunto de servidores consiste en un número de modelos de servidores y el servidor está seleccionado para actualización de BIOS, la lógica del filtro automático quita los demás servidores que no coinciden con el modelo del servidor seleccionado. Esto asegura que la selección de la imagen de actualización del firmware del BIOS (DUP) es compatible con el modelo de servidor correcto.

A veces, la imagen de actualización del firmware del BIOS puede ser compatible con varios modelos. Estas optimizaciones se omiten en caso de que la compatibilidad no continúe en el futuro.

- El filtro automático es importante para actualizaciones de firmware de las controladoras de interfaz de red (NIC) y controladoras RAID. Estas categorías de dispositivos tienen distintos tipos y modelos. De forma parecida, las imágenes de actualización del firmware (DUP) pueden estar disponibles en formularios optimizados en los que un solo DUP podría estar programado para actualizar varios tipos o modelos de dispositivos de una categoría determinada.

La página **Actualización de componentes de servidor** contiene las siguientes secciones:

- Filtro de actualización de componente/dispositivo: esta sección se utiliza para controlar la vista de componentes y dispositivos en la sección **Inventario de firmware**. Al activar el filtro para un tipo de componente o dispositivo, la sección **Inventario de firmware** se modifica para mostrar solo los componentes o dispositivos seleccionados en todos los servidores.

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

Si no se ha seleccionado ningún filtro y se ha seleccionado un componente o dispositivo para su actualización en la sección de inventario, entonces el filtro relacionado con esa selección se activa automáticamente. Puede producirse un filtrado mayor en la parte 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 un componente de BIOS en uno de los servidores está seleccionado 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.

Al activar el filtro se permite filtrar el componente o dispositivo relacionado en la sección **Inventario de firmware**. Después de activar el filtro, solo se pueden ver los componentes o dispositivos relacionados en todos los servidores presentes en el chasis. Se trata de un filtro de paso, lo que significa que solo acepta componentes o dispositivos relacionados con el filtro y excluye a todos los demás. Se pueden seleccionar uno o varios (o todos) filtros según sea necesario.

Los componentes y dispositivos se agrupan en las siguientes categorías:

- BIOS
- iDRAC
- Unified Server Configurator (Lifecycle Controller activado)
- Diagnósticos de 32 bits
- OS-Driver Pack
- Controladores de interfaz de red (NIC) y controladoras RAID
- Inventario de firmware de componentes/dispositivos: esta sección resume el estado de las versiones de firmware de todos los componentes y dispositivos en los servidores que se encuentran actualmente en el chasis. Hay opciones disponibles para realizar las múltiples operaciones de Lifecycle Controller, como Actualizar, Revertir, Reinstalar y Borrar trabajos. Solo puede realizarse un tipo de operación a la vez. Los componentes y dispositivos no admitidos pueden incluirse como parte del inventario, pero no permiten realizar operaciones de Lifecycle Controller.

Los servidores que actualmente no admiten el servicio Lifecycle Controller aparecen como **No admitidos**. Hay un hipervínculo que enlaza con una página alternativa en la que es posible actualizar directamente solo el firmware del iDRAC. Esta página no admite la actualización de ninguno de los componentes o dispositivos en el servidor. Solo puede actualizarse el firmware del iDRAC en esta página alternativa que no depende de Lifecycle Controller.

Si el servidor aparece como **No está listo**, indica que, cuando se recuperó el inventario de firmware, el iDRAC en el servidor estaba todavía inicializándose. Espera a que el iDRAC esté totalmente funcional y actualice la página para recuperar el inventario de firmware otra vez.

Si en el inventario de componentes y dispositivos no aparece lo que está físicamente instalado en el servidor, debe invocar la Unified Server Configurator Console (USC) cuando el servidor está en proceso de inicio. Esto ayuda a actualizar la información de los componentes y dispositivos y proporciona otro medio para verificar lo que está instalado 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.
- Los nuevos dispositivos se acaban de insertar en el servidor.

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

En la consola de inicio de los servidores iDRAC6, cuando aparezca el mensaje Pulsar <Ctrl+E> para Configuración de acceso remoto en 5 s, pulse <Ctrl+E>. Después, en la pantalla 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 Configuración, seleccione Configuración del iDRAC y, después, seleccione Servicios del sistema (USC). En la pantalla Configuración, active **Recolectar inventario del sistema durante el reinicio**.

Tabla 5-59 muestra la información sobre componentes y dispositivos en el servidor:

Tabla 5-59. Información sobre componentes y dispositivos

Campo	Descripción
Ranura	Muestra la ranura ocupada por el servidor en el chasis. Las ranuras son identificaciones consecutivas, de 1 a 16 (de 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 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 dispositivo en el servidor. Si aparece una casilla de verificación al lado de la versión actual, indica que una imagen del firmware instalado actualmente para el componente o dispositivo dentro de Lifecycle Controller está disponible para una operación de Reinstalación .


Tabla 5-59. Información sobre componentes y dispositivos (continuación)

Campo	Descripción
Versión de reversión	Muestra la versión de reversión del componente o dispositivo en el servidor. Si aparece una casilla de verificación al lado de la versión de reversión, indica que una imagen del firmware instalado previamente para el componente o dispositivo dentro de Lifecycle Controller está disponible para una operación de Revertir . La disponibilidad depende de la lógica de compatibilidad de versiones de Lifecycle Controller. Se supone que Lifecycle Controller ha proporcionado la actualización previa.
Estado del trabajo	Muestra el estado del trabajo de cualquier operación programada en el servidor. El estado del trabajo se actualiza continuamente de manera dinámica. Si se detecta un trabajo con el estado completado , las versiones de firmware para los componentes y dispositivos en ese servidor se actualizan automáticamente, por si ha habido algún cambio en la versión de firmware de cualquiera de los componentes o dispositivos. Si aparece una casilla de verificación al lado del estado del trabajo, indica que un trabajo de Lifecycle Controller está en progreso y que se encuentra en el estado indicado . Puede elegirlo para una operación de Eliminar trabajo . Aparece un icono de información al lado del estado actual, que proporciona información adicional sobre el estado de trabajo actual. Esta información se puede consultar si hace clic en el icono o desplaza el mouse sobre él.


Tabla 5-59. Información sobre componentes y dispositivos (continuación)


Campo	Descripción
Actualizar	<p>Selecciona el componente o dispositivo para una actualización de firmware en el servidor. Utilice el acceso directo con la tecla CRTL para seleccionar un tipo de componente o dispositivo para su actualización en todos los servidores aplicables.</p> <p>Al mantener presionada la tecla CRTL se destacan todos los componentes en amarillo. A la vez que presiona la tecla CRTL, seleccione el componente o dispositivo necesario activando la casilla de verificación relacionada en la columna Actualizar.</p> <p>Las actualizaciones del BIOS son específicas al modelo del 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 propia de la funcionalidad de Lifecycle Controller y, particularmente, de la programación en el Dell Update Package (DUP). Actualmente, se admiten Dell Update Packages (DUP) de un tamaño inferior a 48MB.</p> <p>Si el tamaño de la imagen de actualización es mayor, el estado del trabajo indica que se ha producido una falla en la descarga. Si se intentan varias actualizaciones de componentes en un servidor a la vez, el tamaño combinado de todos los archivos de actualización de firmware puede superar los 48MB. En este caso, una de las actualizaciones del componente falla porque su archivo de actualización está truncado. Una estrategia recomendada para actualizar varios componentes en un servidor es primero actualizar juntos el Unified Server Configurator y los componentes de Diagnósticos de 32 bits. No requieren reiniciar el servidor y se completan relativamente rápido. Los demás componentes pueden actualizarse juntos después.</p> <p>Todas las actualizaciones de Lifecycle Controller se programan para ejecutarse inmediatamente. Sin embargo, los servicios del sistema a veces pueden retrasar la ejecución. En estas situaciones, la actualización falla a causa de que el uso compartido remoto que se aloja en el CMC ya no está disponible.</p>

Al seleccionar un componente o dispositivo para su actualización, es necesario especificar el Dell Update Package (DUP). Se muestra una segunda tabla que identifica el componente/dispositivo y un selector del archivo de imagen del firmware. Este permite especificar el archivo de imagen del firmware para el componente o dispositivo relacionado. Se muestra un selector específico para cada tipo de componente/dispositivo que está seleccionado para su actualización.

 **NOTA:** Solo se muestra un selector por categoría de componente o dispositivo.

Esto se nota mejor en los dispositivos de controladoras de interfaz de red (NIC) y los dispositivos de controladoras RAID. Estos dispositivos pueden contener muchos tipos y modelos. La lógica de selección de actualizaciones filtra automáticamente el tipo o modelo de dispositivo relevante según los dispositivos seleccionados inicialmente. La razón principal para este comportamiento de filtro automático es que solo puede especificarse un archivo de imagen del firmware para la categoría. El archivo de imagen del firmware debe ser un Dell Update Package para Microsoft Windows (DUP). Esto es un archivo ejecutable de Microsoft Windows.

 **NOTA:** El límite de tamaño de la actualización equivale a un solo DUP o pueden ignorarse varios DUP combinados si la función Extended Storage (almacenamiento extendido) está instalada y activada. Para obtener información sobre cómo activar el almacenamiento extendido, consulte la sección “Activación de soportes flash extraíbles” en la página 119.

 **NOTA:** Se recomienda borrar la cola de trabajos antes de iniciar una actualización del firmware de los componentes del servidor. En la página **Trabajos de Lifecycle Controller** está disponible 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 en “Administración de trabajos de Lifecycle Controller en un sistema remoto.” en la página 449.

La página **Actualización de componentes de servidor** le permite realizar varias acciones con los botones disponibles. Cada botón realiza la operación relacionada de Lifecycle Controller. Para que se realice una operación, tiene que estar seleccionado como mínimo un componente o dispositivo. Si está seleccionada una operación de **Actualización** para un componente o dispositivo, su archivo de imagen del firmware tiene que especificarse en la sección **Filtro de actualización y Selección de archivo de imagen**. No se desplace a otra página después de enviar una operación para su programación. Si lo intenta, aparecerá un mensaje de confirmación que le permite cancelar el desplazamiento. 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 que indica que la operación se ha programado satisfactoriamente. Una vez 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 el número de reinicios necesarios.

Tabla 5-60 describe los botones disponibles y las acciones que pueden realizarse en la página **Actualización de componentes de servidor**:

Tabla 5-60. Acciones de Actualización de componentes de servidor

Botón	Acción
Actualizar	Realiza la operación de Actualización para programar actualizaciones del firmware de los componentes o dispositivos seleccionados en uno o más servidores.
Reversión	Realiza la operación de Reversión para programar actualizaciones del firmware de los componentes o dispositivos seleccionados para su reversión en uno o más servidores.
Reinstalación	Realiza la operación de Reinstalación para programar reinstalaciones del firmware de los componentes o dispositivos seleccionados en uno o más servidores.
Eliminar trabajo	Realiza la operación Eliminar trabajo para eliminar trabajos relacionados con los componentes o dispositivos seleccionados en uno o más servidores.

En algunos componentes, las acciones Actualización, Reversión y Reinstalación pueden requerir el reinicio del servidor. El reinicio se puede retrasar seleccionando una opción en la lista desplegable. Seleccione **Reiniciar ahora** si es necesario reiniciar el servidor inmediatamente, y **Reiniciar más tarde** para reiniciar el servidor manualmente más adelante.

A veces, 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 que le explica la situación y la operación no se envía. Espere a que termine la operación en curso antes de volver a enviar la otra operación.

Administración del iDRAC

El CMC proporciona la página Implementar iDRAC para permitir al usuario configurar los valores de configuración de red del iDRAC del servidor instalado y recién insertado. Desde esta página, el usuario puede configurar uno o más dispositivos iDRAC instalados. Además, puede configurar los valores predeterminados de la configuración de red del iDRAC y la contraseña raíz para los servidores que se instalarán más adelante; estos valores predeterminados son la configuración de **QuickDeploy de iDRAC**.

Para obtener más información sobre el comportamiento del iDRAC, consulte la *Guía del usuario del iDRAC* en support.dell.com/manuals.

QuickDeploy de iDRAC

La sección **QuickDeploy de iDRAC** de la página **Implementación del iDRAC** tiene los valores de configuración de red que se aplican a los servidores recién insertados. Puede utilizar estos valores para rellenar automáticamente la tabla **Configuración de la red del iDRAC** debajo de la sección **QuickDeploy**. Una vez que se activa **QuickDeploy**, se aplica la configuración de **QuickDeploy** a los servidores cuando se instala el servidor. Para obtener más información sobre la configuración de **QuickDeploy de iDRAC**, consulte el paso 8 de la sección “Configuración del sistema de red por medio del asistente de configuración del panel LCD” en la página 48.

Para activar y definir la configuración de **QuickDeploy de iDRAC**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de servidores** en el árbol del sistema.
- 3 Haga clic en la ficha **Configuración**. Aparece la página **Implementación del iDRAC**.
- 4 Defina los valores de **QuickDeploy** según corresponda.

Tabla 5-61. Configuración de QuickDeploy

Valor	Descripción
QuickDeploy activada	Activa/desactiva la función QuickDeploy que aplica automáticamente los valores del iDRAC configurados en esta página para los servidores recién insertados; la configuración automática <i>debe</i> confirmarse localmente en el panel LCD. NOTA: Esto incluye la contraseña raíz del usuario si se selecciona la casilla Definir contraseña raíz al insertar servidor . Valor predeterminado: sin seleccionar (desactivada)
Definir contraseña raíz del iDRAC al insertar servidor	Especifica si una contraseña raíz del iDRAC del servidor debe cambiarse por el valor proporcionado en el cuadro de texto Contraseña raíz del iDRAC al insertar el servidor.
Contraseña raíz del iDRAC	Cuando se marcan las opciones Definir contraseña raíz del iDRAC al insertar servidor y QuickDeploy activada , este valor de contraseña se asigna a una contraseña raíz del iDRAC al insertar el servidor en el chasis. Las contraseñas pueden tener de 1 a 20 caracteres imprimibles (incluyendo espacios).
Confirmar contraseña raíz del iDRAC	Verifica la contraseña que se introdujo en el campo Contraseña raíz del iDRAC .
Activar LAN del iDRAC	Activa/desactiva el canal LAN del iDRAC. Valor predeterminado: sin seleccionar (desactivado)
Activar el IPv4 del iDRAC	Activa/desactiva el IPv4 en el iDRAC. El valor predeterminado es Activado.
Activar la IPMI en la LAN del iDRAC	Activa/desactiva el canal de la IPMI en la LAN para cada iDRAC presente en el chasis. Valor predeterminado: sin seleccionar (desactivado)
Activar DHCP del iDRAC	Activa/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 estas configuraciones para cada iDRAC. Valor predeterminado: sin seleccionar (desactivado)

Tabla 5-61. Configuración de QuickDeploy (continuación)

Valor	Descripción
Dirección IPv4 inicial del iDRAC (ranura 1)	<p>Especifica la dirección IP estática del iDRAC del servidor en la ranura 1 del gabinete. La dirección IP de cada iDRAC subsiguiente incrementa 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 el número de ranura sea mayor que la máscara de subred, se mostrará un mensaje de error.</p> <p>NOTA: La máscara de subred y la puerta de enlace no se incrementan como la dirección IP.</p> <p>Por ejemplo, si la dirección IP inicial es 192.168.0.250 y la máscara de subred es 255.255.0.0, entonces 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 El rango de direcciones IP de QuickDeploy no se encuentra completamente dentro de la subred de QuickDeploy al presionar el botón Guardar configuración de QuickDeploy o el botón Completar automáticamente usando la configuración de QuickDeploy.</p>
Máscara de red IPv4 del iDRAC	Especifica la máscara de subred de QuickDeploy que se asigna a todos los servidores nuevos 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 el IPv6 del iDRAC	Activa la dirección IPv6 de cada iDRAC presente en el chasis que es compatible con IPv6.
Activar la configuración automática del IPv6 del iDRAC	Permite que el iDRAC obtenga la configuración de IPv6 (dirección y longitud de prefijo) de un servidor DHCPv6 y también activa la configuración automática de dirección sin estado. El valor predeterminado es Activado.
Puerta de enlace IPv6 del iDRAC	Especifica la puerta de enlace IPv6 predeterminada para asignar 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.

- 5 Para guardar las selecciones, haga clic en el botón **Guardar configuración de QuickDeploy**. Si realizó cambios en la configuración de red del iDRAC, haga clic en el botón **Aplicar configuración de red del iDRAC** para implementar la configuración en el iDRAC.
- 6 Para actualizar la tabla a la configuración de QuickDeploy guardada más reciente y restaurar los valores actuales de configuración de red del iDRAC de cada servidor instalado, haga clic en el botón **Actualizar**.



NOTA: Al hacer clic en el botón **Actualizar** se eliminan todas las configuraciones de QuickDeploy de iDRAC y de red del iDRAC que no se hayan guardado.

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 de IPMI en la 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 de DHCP.

Para copiar la configuración de QuickDeploy a la sección **Configuración de la red del iDRAC**, haga clic en **Completar automáticamente usando la configuración de QuickDeploy**. Los valores de configuración de red de QuickDeploy se copian en los campos correspondientes en la tabla **Valores de configuración de red del iDRAC**.



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

Configuración de la red de iDRAC

La sección **Configuración de la red del iDRAC** de la página **Implementación del iDRAC** tiene una tabla que contiene todos los valores de configuración de red IPv4 e IPv6 del iDRAC de todos los servidores instalados. Con esta tabla se pueden definir los valores de configuración de red del iDRAC de 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. Al cambiar un campo y hacer clic en **Aplicar configuración de la red del iDRAC** se guarda el campo modificado en el iDRAC.

Para activar y definir la configuración de red de iDRAC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de servidores** en el árbol del sistema.
- 3 Haga clic en la ficha **Configuración**.
Aparece la página **Implementación del iDRAC**.
- 4 Seleccione la casilla para **QuickDeploy activada** para activar la configuración de QuickDeploy.
- 5 Defina la **Configuración de la red del iDRAC** según corresponda.

Tabla 5-62. Configuración de la red de iDRAC

Valor	Descripción
Ranura	Muestra la ranura ocupada por el servidor en el chasis. Los números de las ranuras son identificaciones progresivas, de 1 a 16 (hay 16 ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis. NOTA: 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. De manera predeterminada, las ranuras se denominan SLOT-01 a SLOT-16. NOTA: El nombre de ranura no puede ser nulo ni dejarse en blanco.
Activar LAN	Activa (seleccionado) o desactiva (deseleccionado) el canal LAN. NOTA: Cuando no se selecciona LAN (desactivado), no se utilizan todas las otras configuraciones de red (IPMI en la LAN, DHCP, Máscara de subred de dirección IP y Puerta de enlace). No se puede tener acceso a estos campos.
Cambiar contraseña raíz	Activa (cuando se selecciona) la capacidad de cambiar la contraseña del usuario raíz del iDRAC. Los campos Contraseña raíz del iDRAC y Confirmar contraseña raíz del iDRAC deben proporcionarse para que la operación se realice satisfactoriamente.

Tabla 5-62. Configuración de la red de iDRAC (continuación)

Valor	Descripción
DHCP	Si se selecciona, DHCP se utilizan para adquirir la dirección IP del iDRAC, la máscara de subred y la puerta de enlace predeterminada, de lo contrario se utilizan los valores definidos en los campos de configuración de red del iDRAC. Es necesario activar la LAN para definir este campo.
IPMI en la LAN	Activa (seleccionado) o desactiva (deseleccionado) el canal IPMI en la LAN. Es necesario activar la LAN para definir este campo.
Dirección IP	La dirección IPv4 o IPv6 estática asignada al iDRAC que se encuentra en esta ranura.
Máscara de subred	Especifica la máscara de subred asignada al iDRAC instalado en esta ranura.
Puerta de enlace	Especifica la puerta de enlace predeterminada asignada al iDRAC que se instalará en esta ranura.
Activar IPv4	Permite que el iDRAC de la ranura utilice el protocolo IPv4 en la red. Se debe seleccionar la opción Activar LAN para que esta opción esté activada. El valor predeterminado es Activado.
Activar IPv6	Permite que el iDRAC de la ranura utilice el protocolo IPv6 en la red. Se debe seleccionar la opción Activar LAN y dejar en blanco la opción Configuración automática para que esta opción esté activada. La configuración predeterminada es Desactivada. NOTA: Esta opción estará disponible solamente si el servidor es compatible con IPv6.
Configuración automática	Permite que el iDRAC obtenga la configuración de IPv6 (dirección y longitud de prefijo) de un servidor DHCPv6 y también activa la configuración automática de dirección sin estado. NOTA: Esta opción estará disponible solamente si el servidor es compatible con IPv6.
Longitud del prefijo	Especifica la longitud, en bits, de la subred IPv6 a la cual pertenece este iDRAC.

- 6 Para implementar la configuración en iDRAC, haga clic en el botón **Aplicar configuración de red del iDRAC**. Si se realizaron cambios en la configuración de QuickDeploy, estos también se guardarán.
- 7 Para restaurar los valores actuales de la configuración de red del iDRAC para cada servidor instalado y actualizar la tabla de QuickDeploy con la configuración guardada más reciente, haga clic en **Actualizar**.



NOTA: Al hacer clic en el botón **Actualizar** se eliminan todos los valores de configuración de QuickDeploy y de red del iDRAC que no se hayan guardado.

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. Presione el botón **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 más valores de configuración de red del servidor iDRAC pueden requerir un par de minutos para propagarse desde el CMC a un iDRAC. Si se presiona el botón **Actualizar** demasiado rápido, es posible que solo se muestren datos parcialmente correctos de uno o más servidores iDRAC.

Inicio de la consola remota desde la interfaz gráfica de usuario de CMC

Esta función permite iniciar una sesión de teclado, video y mouse (KVM) directamente en el servidor.

Para iniciar la consola remota del servidor desde la página de inicio de la interfaz gráfica de usuario del CMC:

- 1 Haga clic en el servidor específico en el gráfico del chasis.
- 2 En **Vínculos de acceso rápido**, haga clic en el vínculo **Iniciar la consola remota**.

Para iniciar la consola remota del servidor desde la página **Estado de los servidores**:

- 1 En el árbol del sistema, seleccione **Descripción general de servidores**.
- 2 Haga clic en **Iniciar la consola remota** en la tabla del servidor especificado.

Para iniciar la consola remota de un servidor individual:

- 1 Expanda la opción **Descripción general de servidores** en el árbol del sistema. Todos los servidores (1 a 16) aparecen en la lista expandida de servidores.
- 2 En el árbol del sistema, haga clic en el servidor que desea ver. Aparecerá la página **Estado del servidor**.
- 3 Haga clic en **Iniciar la consola remota**.

La consola remota solo se admite cuando se cumplen todas las condiciones siguientes:

- El chasis está encendido.
- Servidores que 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).



NOTA: La consola remota también puede abrirse desde la interfaz gráfica de usuario del iDRAC. Consulte la interfaz gráfica de usuario del iDRAC para obtener más información.

Cómo iniciar el iDRAC mediante el inicio de sesión único

El CMC proporciona administración limitada de componentes individuales del chasis, tales como 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).

Para iniciar la consola de administración de iDRAC desde la página de **Servidores** haga lo siguiente:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de servidores** en el árbol del sistema. Aparece la página **Estado de los servidores**.
- 3 Haga clic en el botón **Iniciar interfaz gráfica de usuario del iDRAC** del servidor que desea administrar.

Para iniciar la consola de administración del iDRAC de un servidor individual:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Expanda la opción **Descripción general de servidores** en el árbol del sistema. Todos los servidores (1 a 16) aparecen en la lista expandida de **Servidores**.
- 3 Haga clic en el servidor que desea ver. Aparecerá la página **Estado del servidor**.
- 4 Haga clic en el botón **Iniciar interfaz gráfica de usuario del iDRAC**.

Un usuario puede iniciar la interfaz gráfica de usuario del iDRAC sin tener que iniciar sesión por segunda vez, debido a que esta función utiliza inicio de sesión único. Las políticas de inicio de sesión único se describen a continuación.

- Un usuario de CMC con privilegio administrativo de servidor se conectará automáticamente con iDRAC mediante inicio de sesión único. Una vez que se encuentra en el sitio iDRAC, se otorgan privilegios de administrador a este usuario automáticamente. Esto sucede aunque el usuario no tenga una cuenta en iDRAC, o si la cuenta no tiene privilegios de administrador.
- Un usuario del CMC que **NO** tenga privilegio administrativo de servidor, pero que tenga la misma cuenta en iDRAC, se conectará automáticamente con iDRAC mediante inicio de sesión único. Una vez que se encuentra en el sitio iDRAC, se otorgan privilegios a este usuario que fueron creados para la cuenta iDRAC.
- Un usuario del CMC que no tenga privilegio administrativo de servidor, o la misma cuenta en iDRAC, **NO** se conectará automáticamente con iDRAC mediante inicio de sesión único. Este usuario se envía a la página de inicio de sesión de iDRAC al hacer clic en el botón **Iniciar interfaz gráfica de usuario del iDRAC**.



NOTA: El término “la misma cuenta” en este contexto significa que el usuario tiene el mismo nombre de inicio de sesión con una contraseña que coincide para CMC y para iDRAC. Cuando el usuario tenga el mismo nombre de inicio de sesión pero sin una contraseña que coincida, no se considerará que tiene la misma cuenta.



NOTA: Se puede pedir a los usuarios que se conecten con 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.



NOTA: 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 el icono Iniciar interfaz gráfica de usuario del iDRAC.

Clonación de servidores

La función de clonación de servidores permite al usuario aplicar todos los valores clonables del BIOS de un servidor específico en uno o varios servidores. Los valores clonables del BIOS son aquellos que se pueden modificar y están pensados para su replicación en varios servidores.

Esta función admite servidores iDRAC6 e iDRAC7. Los servidores iDRAC de la generación anterior se muestran, aunque en la página principal están desactivados y no pueden utilizar esta función.

Para utilizar la función de clonación de servidores:

- Debe tener la versión mínima requerida del iDRAC. Los servidores iDRAC6 requieren como mínimo la versión 3.2 y los servidores iDRAC7, la versión 1.0.0.
- El servidor debe tener la generación admitida de iDRAC.
- El servidor debe estar encendido.

Los valores del BIOS solo se pueden configurar con la función de clonación de servidores a través de la interfaz web del CMC. Esta operación se puede realizar en la página Perfiles del BIOS.

Para acceder a la página Perfiles del BIOS, haga clic en **Descripción general de servidores**→ **Configuración**→ **Perfiles**.

Los servidores de origen y destino no son de la misma generación. Solo se aplican a otros servidores los valores clonables disponibles de un perfil de servidor.

Captura de perfiles

Antes de clonar las propiedades del BIOS de un servidor, debe capturarlas en un Perfil almacenado.

Cuando cree un Perfil almacenado, debe proporcionar un nombre y una descripción opcional para cada perfil. En el soporte de almacenamiento extendido no volátil del CMC se puede guardar un máximo de 16 perfiles almacenados.

La eliminación o desactivación del soporte de almacenamiento extendido no volátil impide el acceso a los perfiles almacenados, y desactiva la función Clonación de servidores.

Aplicación de perfiles

Para iniciar una operación de clonación de servidores cuando hay perfiles almacenados disponibles en el soporte no volátil del CMC, aplique un perfil almacenado a uno o varios servidores.

El estado de la operación, número de ranura, nombre de ranura y nombre de modelo de cada servidor se muestran en la tabla **Aplicar perfil**. Después de aplicar un perfil almacenado a un servidor, este se reinicia inmediatamente.

Visualización de la configuración del BIOS en el servidor

Para ver los valores del BIOS de un servidor determinado en la tabla **Aplicar perfil**, haga clic en **Ver** en la columna Valores del BIOS de la entrada seleccionada.

Se mostrará la página **Ver configuración**.

Solo se muestran los valores del BIOS del servidor que se pueden modificar aplicando un perfil (valores clonables). Los valores se dividen en grupos de manera similar a cómo se muestran en la pantalla Configuración del BIOS del iDRAC.



NOTA: Los cambios realizados en la configuración del BIOS de la blade en la consola no se muestran en la página **Ver configuración** hasta que se realiza un inventario del sistema en la blade. Para ello, debe estar activar en el BIOS la opción **Recopilar inventario del sistema al reiniciar (CSIOR)**.

Gestión de perfiles almacenados

Para administrar los perfiles almacenados en el CMC, haga clic en **Administrar perfiles** en la tabla **Aplicar perfil**. Se mostrará la página **Administrar perfiles del BIOS**.

En la página **Administrar perfiles del BIOS**, puede editar el nombre o descripción de un perfil almacenado, ver los valores del BIOS que contiene o eliminar un perfil almacenado.

Registro de perfiles recientes

En la tabla **Registro de perfiles recientes** de la página principal de clonación blade se enumeran las entradas del registro de perfiles recientes procedentes directamente de las operaciones de clonación de servidores. Cada registro muestra la gravedad, la hora y la fecha en que se envió la operación de clonación de servidores, y la descripción del mensaje de registro de clonación.

Los mensajes de la tabla **Registro de perfiles recientes** también se incluyen en el registro de RAC. La tabla Registro de perfiles recientes muestra las 10 últimas entradas del registro de perfiles. Para ver las demás entradas disponibles, haga clic en **Ir al registro de perfiles**.

Estado de compleción y solución de problemas

Para comprobar el estado de compleción de un perfil de BIOS solicitado aplicado:

- 1 Capture el Id. de trabajo (JID) del trabajo enviado que desee en la tabla **Registro de perfiles recientes** disponible en la página principal de clonación de servidores.
- 2 Busque el mismo JID en la tabla **Trabajos** de la página **Trabajos de Lifecycle Controller (Descripción general de servidores→ Solución de problemas→ Trabajos de Lifecycle Controller)**.

FlexAddress

Esta sección describe las pantallas de la interfaz web de FlexAddress. FlexAddress es una actualización opcional que permite que los módulos de los servidores reemplacen la identificación WWN/MAC asignada en fábrica por una identificación WWN/MAC proporcionada por el chasis.



NOTA: Es necesario adquirir e instalar la actualización FlexAddress para tener acceso a las pantallas de configuración. Si no se adquirió e instaló la actualización, aparecerá el siguiente texto en la interfaz web:

Función opcional no instalada. Consulte la información de la *Guía del usuario de Dell Chassis Management Controller* para obtener información acerca de la función de administración de direcciones WWN y MAC basadas en el chasis.

Para adquirir esta función, póngase en contacto con Dell en www.dell.com.

Cómo ver el estado de FlexAddress

Puede utilizar la interfaz web para ver información del estado de FlexAddress. Puede ver información del estado del chasis completo o de un servidor individual. La información que se muestra incluye:

- Configuración de la red Fabric.
- FlexAddress activado/no activado.
- Número y nombre de la ranura.
- Direcciones asignadas por el chasis y por el servidor.
- Direcciones en uso.



NOTA: También puede ver el estado de FlexAddress a través de la interfaz de la línea de comandos. Para obtener más información acerca de los comandos, ver “Uso de FlexAddress” en la página 257.

Cómo ver el estado de FlexAddress del chasis

La información del estado de FlexAddress se puede mostrar para todo el chasis. La información de estado incluye datos para saber si la función está activada y una descripción general del estado de FlexAddress de cada servidor.

Para comprobar si la FlexAddress del chasis está activa haga lo siguiente:

- 1 Inicie sesión en la interfaz web (ver “Acceso a la interfaz web del CMC” en la página 115).
- 2 Haga clic en **Descripción general del chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración general**. La anotación de FlexAddress tendrá un valor de **Activado** o **No activado**; el valor activado significa que la función está instalada en el chasis. El valor no activado significa que la función no está instalada y no se está utilizando en el chasis.

Haga lo siguiente para mostrar una descripción general de FlexAddress en cada módulo de servidor:

- 1 Inicie sesión en la interfaz web (“Acceso a la interfaz web del CMC” en la página 115).
- 2 Haga clic en **Descripción general de servidores**→ **Propiedades**→ **WWN/MAC**.

- 3** Aparecerá la página **Resumen de FlexAddress**. Esta página le permite ver la configuración de WWN y las direcciones MAC de todas las ranuras del chasis.

La página de estado presenta la siguiente información:

Configuración de la red Fabric	<p>Red Fabric A, Red Fabric B y Red Fabric C muestran los tipos de red Fabric de entrada/salida instalados.</p> <p>iDRAC muestra la dirección MAC de administración del servidor.</p> <p>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 direcciones MAC o WWN para las redes Fabric B y C si están siendo utilizadas por ranuras ocupadas.</p>
Direcciones WWN/MAC	<p>Muestra la configuración de FlexAddress para cada ranura del chasis. La información que se muestra incluye:</p> <ul style="list-style-type: none">• La controladora de administración del iDRAC no es una red Fabric pero el FlexAddress de este se trata como si lo fuera.• Número y ubicación de la ranura• Estado de FlexAddress activado/no activado• Tipo de red Fabric• Direcciones WWN/MAC en uso asignadas por el servidor y por el chasis. <p>Una marca verde indica el tipo de dirección activada, ya sea asignada por el servidor o por el chasis.</p>

- 4** Para obtener más información, haga clic en **Ayuda**.

Cómo ver el estado de FlexAddress del servidor

La información del estado de FlexAddress también se puede mostrar para cada servidor individual. La información de nivel de servidor muestra una descripción general del estado de FlexAddress para ese servidor.

Para ver la información del servidor de FlexAddress haga lo siguiente:





- 1** Inicie sesión en la interfaz web (ver “Acceso a la interfaz web del CMC” en la página 115).
- 2** Expanda la opción **Descripción general de servidores** en el árbol del sistema. Todos los servidores (1 a 16) aparecen en la lista expandida de **Servidores**.

- 3 Haga clic en el servidor que desea ver.
Aparecerá la página **Estado del servidor**.
- 4 Haga clic en la ficha **Configuración** y en la subficha **FlexAddress**.
Aparecerá la página **Implementar FlexAddress**. Esta página le permite ver la configuración de WWN y las direcciones MAC del servidor seleccionado.
La página de estado presenta la siguiente información:

Tabla 5-63. Información de página de estado

FlexAddress activado	Muestra si la función FlexAddress está activada o no para la ranura específica.
Estado actual	Muestra la configuración actual de FlexAddress: <ul style="list-style-type: none"> • Asignada por el chasis: la dirección de la ranura seleccionada es asignada por el chasis a través de FlexAddress. Las direcciones WWN/MAC basadas en la ranura son las mismas aun si se instala un nuevo servidor. • Asignada por el servidor: el servidor utiliza la dirección asignada por el servidor o la dirección predeterminada incorporada en el hardware de la controladora.
Estado de la alimentación	Muestra el estado actual de la alimentación de los servidores. Los valores son: On (encendido), Powering On (encendiendo), Powering Off (apagando), Off (apagado) y N/A (N/D), si no hay un servidor presente.

Tabla 5-63. Información de página de estado (continuación)

Condición		En buen estado	Indica que FlexAddress está presente y proporciona el estado al CMC. En caso de una falla de comunicación entre el CMC y FlexAddress, el CMC no puede obtener ni mostrar el estado de FlexAddress.
		Información	Muestra información acerca de FlexAddress cuando no se ha producido ningún cambio en el estado de la condición (En buen estado, Advertencia, Crítico).
		Aviso	Muestra que solo se emitieron alertas de aviso que deben tomarse medidas correctivas . Si no se toman medidas correctivas, existe la posibilidad de que surjan fallas críticas que pueden afectar la integridad del servidor.
		Crítico	Muestra que se ha enviado al menos una alerta de falla. El estado crítico representa una falla del sistema en el servidor y se debe tomar una medida correctiva de inmediato .
		Sin valor	Cuando FlexAddress está ausente, no se proporciona información sobre la condición.
Firmware del iDRAC	Muestra la versión del iDRAC instalada actualmente en el servidor.		
Versión del BIOS	Muestra la versión actual del BIOS del módulo de servidores.		
Ranura	Número de ranura del servidor asociado con la ubicación de la red Fabric.		
Ubicación	Muestra la ubicación del módulo de E/S de entrada/salida en el chasis por número de grupo (A, B o C) y por número de ranura (1 ó 2). Nombres de las ranuras: A1, A2, B1, B2, C1 o C2.		
Red Fabric	Muestra el tipo de red Fabric.		
Asignada por el servidor	Muestra las direcciones WWN/MAC asignadas por el servidor integradas en el hardware de la controladora.		
Asignada por el chasis	Muestra las direcciones WWN/MAC asignadas por el chasis que se utilizan para la ranura específica.		

5 Para obtener más información, haga clic en **Ayuda**.

Configuración de FlexAddress

Si ha adquirido FlexAddress con el chasis, se instalará y activará al encender el sistema. Si ha adquirido FlexAddress por separado, deberá instalar la tarjeta de función SD según las instrucciones del documento *Especificaciones técnicas de la tarjeta Secure Digital (SD) de Chassis Management Controller (CMC)*. Ver support.dell.com/manuals para obtener este documento.

El servidor debe estar apagado antes de comenzar la configuración. Puede activar o desactivar FlexAddress por red Fabric. Además, puede activar/desactivar la función por ranura. Después de haber activado la función por red Fabric, puede seleccionar las ranuras que se activarán. Por ejemplo, si la red Fabric A está activada, todas las ranuras que estén activadas tendrán FlexAddress activado solo en la red Fabric A. El resto de las redes Fabric utilizarán la WWN/MAC asignada de fábrica en el servidor.

Las ranuras seleccionadas tendrán FlexAddress activado para todas las redes Fabric activadas. Por ejemplo, no es posible activar la red Fabric A y B y tener la ranura 1 con FlexAddress activado en la red Fabric A pero no en la red Fabric B.



NOTA: También puede configurar FlexAddress a través de la interfaz de línea de comandos. Para obtener más información acerca de los comandos, ver “Uso de FlexAddress” en la página 257.



NOTA: Asegúrese de que los servidores blade estén apagados antes de cambiar la dirección flexible de nivel de Fabric (A, B, C o DRAC).

Configuración FlexAddress para ranuras y redes Fabric a 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 seleccionarán las ranuras para su participación en la función. Tanto las redes Fabric como las ranuras deben activarse para configurar FlexAddress satisfactoriamente.

Realice los siguientes pasos para activar o desactivar las redes Fabric y las ranuras para utilizar la función FlexAddress:

- 1 Inicie sesión en la interfaz web (ver “Acceso a la interfaz web del CMC” en la página 115).
- 2 Haga clic en **Descripción general de servidores** en el árbol del sistema.
- 3 Haga clic en la ficha **Configuración** → subficha **FlexAddress**. Aparecerá la página **Implementar FlexAddress**.

- 4 La página **Seleccionar redes Fabric para WWN/MAC asignadas por el chasis** muestra una casilla para **Red Fabric A**, **Red Fabric B**, **Red Fabric C** e **iDRAC**.
- 5 Haga clic en la casilla de cada red Fabric en la que desee activar FlexAddress. Para desactivar una red Fabric, haga clic en la casilla para deseleccionarla.



NOTA: Si no se seleccionan las redes Fabric, FlexAddress no estará activado para las ranuras seleccionadas.

La página **Seleccionar ranuras para WWN/MAC asignadas por el chasis** muestra la casilla **Activado** para cada ranura en el chasis (1-16).

- 6 Haga clic en la casilla **Activado** de cada ranura para la que desea activar FlexAddress. Si desea seleccionar todas las ranuras, utilice la casilla **Seleccionar/Deseleccionar todo**. Para desactivar una ranura, haga clic en la casilla **Activado** para deseleccionarla.



NOTA: Si el servidor está presente en la ranura, debe ser apagado antes de que se active la función FlexAddress en esa ranura.



NOTA: Si no se selecciona ninguna ranura, FlexAddress no estará activado para las redes Fabric seleccionadas.

- 7 Haga clic en **Aplicar** para guardar los cambios. Para obtener más información, haga clic en **Ayuda**.

Configuración de FlexAddress de ranuras a nivel del servidor

En el nivel del servidor, puede activar o desactivar la función FlexAddress para ranuras individuales.

Para activar o desactivar una única ranura para que utilice la función FlexAddress, haga lo siguiente:

- 1 Inicie sesión en la interfaz web (ver “Acceso a la interfaz web del CMC” en la página 115).
- 2 Expanda la opción **Descripción general de servidores** en el árbol del sistema. Todos los servidores (1 a 16) aparecen en la lista expandida de **Servidores**.
- 3 Haga clic en el servidor que desea ver. Aparecerá la página **Estado del servidor**.

- 4 Haga clic en la ficha **Configuración** y en la subficha **FlexAddress**. Aparecerá la página **Estado de FlexAddress**.
- 5 Utilice el menú desplegable de **FlexAddress activado** para realizar la selección; seleccione **Sí** para activar FlexAddress o seleccione **No** para desactivar FlexAddress.
- 6 Haga clic en **Aplicar** para guardar los cambios. Para obtener más información, haga clic en **Ayuda**.

Uso compartido de archivos remotos

La opción Uso compartido de archivos de soportes virtuales remotos asigna un archivo de una unidad compartida de la red a uno o más servidores a través del CMC para implementar o actualizar un sistema operativo. Cuando se conecta, se puede acceder al archivo remoto como si estuviera en el sistema local. Es compatible con dos tipos de soportes: Unidades de disco flexible y unidades de CD/DVD.

- 1 Inicie sesión en la interfaz web (ver “Acceso a la interfaz web del CMC” en la página 115).
- 2 Haga clic en **Descripción general de servidores** en el árbol del sistema.
- 3 Haga clic en la ficha **Configuración** y en la subficha **Uso compartido de archivos remotos**. Se muestra la página **Implementar recurso compartido de archivos remotos**.
- 4 Establezca la configuración del uso compartido de archivos remotos.

Tabla 5-64. Configuración de uso compartido de archivos remotos


Valor	Descripción
Ruta de acceso del archivo de imagen	<p>La ruta de acceso del archivo de imagen solamente es necesaria para las operaciones de conexión e implementación. No se aplica a las operaciones de desconexión. El nombre de la ruta de acceso de la unidad de red se monta en el servidor mediante un protocolo Windows SMB o Linux/Unix NFS.</p> <p>Por ejemplo, para conectarse a CIFS escriba:</p> <pre>//<IP para conexión para sistema de archivos CIFS>/<ruta de archivo>/<nombre de imagen></pre> <p>Para conectarse a NFS escriba:</p> <pre>//<IP para conexión para sistema de archivos> : /<ruta de archivo>/<nombre de imagen>name</pre> <p>Los nombres de archivos que terminan en .img se conectan como discos flexibles virtuales. Los nombres de archivo que terminan en .iso se conectan como CD/DVD virtuales. El número máximo de caracteres es 511.</p>
Nombre de usuario	<p>El nombre de usuario se necesita solamente para las operaciones de conexión e implementación. No se aplica a las operaciones de desconexión. El número máximo de caracteres que se pueden especificar en este campo es 40.</p>
Contraseña	<p>La contraseña se necesita solamente para las operaciones de conexión e implementación. No se aplica a las operaciones de desconexión. El número máximo de caracteres que se pueden especificar en este campo es 40.</p>
Ranura	<p>Identifica la ubicación de la ranura. Los números de ranura son consecutivos de 1 a 16 (para las 16 ranuras disponibles del chasis).</p>
Nombre	<p>Muestra el nombre de la ranura. El nombre de la ranura depende de su posición en el chasis.</p>
Modelo	<p>Muestra el nombre de modelo del servidor.</p>

Tabla 5-64. Configuración de uso compartido de archivos remotos (continuación)

Valor	Descripción
Estado de la alimentación	Muestra el estado de la alimentación del servidor: N/A: el CMC no ha determinado aún el estado de la alimentación del servidor. Apagado: el servidor, o el chasis, está apagado. Encendido: tanto el chasis como el servidor están encendidos. Encendiendo: estado temporal entre Apagado y Encendido. Al concluir, el estado es Encendido. Apagando: estado temporal entre Encendido y Apagado. Al concluir, el estado es Apagado.
Estado de conexión	Muestra el estado de conexión del recurso compartido de archivos remotos.
Seleccionar/ Deseleccionar todo	Seleccione esta opción antes de iniciar una operación del recurso compartido de archivos remotos. Las operaciones del recurso compartido de archivos remotos son: Conectar, Desconectar e Implementar.

- 5 Haga clic en **Conectar** para conectarse a un recurso compartido de archivos remotos. Para conectarse a un recurso compartido de archivos remotos, debe proporcionar la ruta de acceso, el nombre de usuario y la contraseña. La operación satisfactoria permitirá acceder a los soportes. Haga clic en **Desconectar** para desconectarse de un recurso compartido de archivos remotos que se conectó anteriormente.

Haga clic en **Implementar** para implementar el dispositivo de soportes.

 **NOTA:** Guarde todos los archivos de trabajo antes de ejecutar el comando **Implementar** porque esta acción hace que el servidor se reinicie.

Este comando involucra estas acciones:

- 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.

Preguntas frecuentes

La Tabla 5-65 muestra las preguntas frecuentes relacionadas con la administración o recuperación de un sistema remoto.

Tabla 5-65. Administración y recuperación de un sistema remoto

Pregunta	Respuesta
Al acceder a la interfaz web del CMC, recibo un aviso de seguridad que indica que el nombre del host del certificado SSL no coincide con el nombre del host del CMC.	<p>El CMC incluye un certificado de servidor del CMC predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Cuando se utiliza este certificado, el explorador de web muestra un aviso de seguridad porque el certificado predeterminado se emite para el Certificado predeterminado del CMC, que no coincide con el nombre de host del CMC (por ejemplo, la dirección IP).</p> <p>Para resolver 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 registrado del CMC de DNS.</p> <p>Para asegurarse de que la CSR coincida con el nombre DNS registrado del CMC:</p> <ol style="list-style-type: none">1 En el árbol Sistema, haga clic en Descripción general del chasis.2 Haga clic en la ficha Red y luego haga clic en Red. Aparecerá la página Configuración de la red.3 Seleccione la casilla Registrar el CMC en DNS.4 Introduzca el nombre del CMC en el campo Nombre del CMC de DNS.5 Haga clic en Aplicar cambios. <p>Para obtener más información acerca de cómo producir CSR y cómo emitir certificados, ver “Protección de las comunicaciones del CMC con certificados SSL y digitales” en la página 193.</p>

Tabla 5-65. Administración y recuperación de un sistema remoto (continuación)

Pregunta	Respuesta
¿Por qué no están disponibles RACADM remoto y los servicios web después de un cambio de propiedad?	<p data-bbox="460 280 960 395">Es posible que los servicios de RACADM remoto y de la interfaz web tarden un minuto para estar disponibles después de que el servidor de web del CMC se restablezca.</p> <p data-bbox="460 408 960 464">El servidor de web del CMC se restablece después de los siguientes acontecimientos:</p> <ul data-bbox="460 480 960 839" style="list-style-type: none"><li data-bbox="460 480 960 563">• Cuando se cambia la configuración de la red o las propiedades de seguridad de la red por medio de la interfaz de usuario de web del CMC.<li data-bbox="460 579 960 662">• Cuando la propiedad <code>cfgRacTuneHttpsPort</code> cambia (incluso cuando un comando <code>config -f <archivo de config></code> la cambia).<li data-bbox="460 678 960 732">• Cuando se utiliza <code>racresetcfg</code> o se restablece una copia de seguridad de la configuración del chasis.<li data-bbox="460 748 960 772">• Cuando el CMC se restablece.<li data-bbox="460 788 960 839">• Cuando se carga un nuevo certificado de servidor SSL.
¿Por qué mi servidor DNS no registra mi CMC?	<p data-bbox="460 860 900 916">Algunos de los servidores DNS solo registran nombres de 31 caracteres o menos.</p>
Al acceder a la interfaz web del CMC, recibo un aviso de seguridad que indica que el certificado SSL fue emitido por una autoridad de certificados que no es confiable.	<p data-bbox="460 932 960 1281">El CMC incluye un certificado de servidor del CMC predeterminado para garantizar la seguridad de la red para las funciones de la interfaz web y de RACADM remoto. Este certificado <i>no</i> es emitido por una autoridad de certificados confiable. Para resolver 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, ver “Protección de las comunicaciones del CMC con certificados SSL y digitales” en la página 193.</p>

Tabla 5-65. Administración y recuperación de un sistema remoto (continuación)

Pregunta	Respuesta
El mensaje siguiente se muestra por motivos desconocidos: Acceso remoto: Fallo de autenticación de SNMP ¿Por qué sucede esto?	<p>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” (público). Cuando IT Assistant envía una solicitud de comunidad Set, el agente CMC genera el error de autenticación SNMP porque solo acepta solicitudes de comunidad = public.</p> <p>Puede cambiar el nombre de comunidad del CMC por medio de RACADM.</p> <p>Para ver el nombre de comunidad del CMC, utilice el comando siguiente:</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>Para establecer el nombre de comunidad del CMC, utilice el comando siguiente:</p> <pre>racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nombre de comunidad></pre> <p>Para evitar que se generen capturas de autenticación 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.</p>

Solución de problemas del CMC

La interfaz web del CMC proporciona herramientas para identificar, diagnosticar y corregir problemas del chasis. Para obtener más información acerca de la solución de problemas, ver “Solución de problemas y recuperación” en la página 429.

Uso de FlexAddress

La función FlexAddress es una actualización opcional que permite a los módulos del servidor reemplazar las identificaciones de red Nombre a nivel mundial y Control de acceso al medio (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 dar cuenta del nuevo módulo del servidor.

FlexAddress permite a CMC asignar identificaciones WWN/MAC a una ranura determinada y *reemplazar* las identificaciones de fábrica. Si se sustituye el módulo de servidor, las identificaciones WWN/MAC basadas en ranuras continúan siendo las mismas. Con esta función, ya no es necesario volver a configurar las herramientas de administración de red Ethernet ni los recursos de SAN para un nuevo módulo del servidor.

Además, la acción de *reemplazo* solo se produce si se inserta el módulo de servidor en un chasis activado para FlexAddress; no se realiza ningún cambio permanente en el módulo del servidor. Si se traslada un módulo de servidor a un chasis que no es compatible con FlexAddress, se utilizarán las Id. WWN/MAC asignadas de fábrica.

Antes de instalar FlexAddress, puede determinar el rango de direcciones MAC contenidas en una tarjeta de función FlexAddress mediante la inserción de la tarjeta SD en un lector de tarjetas de memoria USB y la consulta el archivo `pwwn_mac.xml`. Este archivo XML de texto no cifrado de la tarjeta SD contendrá una etiqueta XML `mac_start`, que es la primera dirección MAC hexadecimal inicial que se utilizará para este intervalo exclusivo de direcciones MAC. La etiqueta `mac_count` es el número total de direcciones MAC asignadas por la tarjeta SD. El rango de MAC totales asignadas se puede determinar mediante:

$$\langle mac_start \rangle + 0xCF (208 - 1) = mac_end$$

donde 208 es `mac_count` y la fórmula es

$$\langle mac_start \rangle + \langle mac_count \rangle - 1 = \langle mac_end \rangle$$

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.*

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

Componente	Versión mínima necesaria
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 cuando se reinicia el CMC con la tarjeta de función SD instalada; esta activación hará que la función se vincule al chasis actual. Si tiene la tarjeta SD instalada en el CMC redundante, la activación de la función FlexAddress no se producirá sino hasta que se active 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 activar un CMC redundante.

Al reiniciar el CMC, verifique el proceso de activación mediante los pasos que se explican en la próxima sección, “Verificación de la activación de FlexAddress” en la página 260.

Verificación de la activación de FlexAddress

Para asegurar la activación adecuada de FlexAddress, se pueden utilizar los comandos de RACADM para verificar la tarjeta de función SD y la activación de FlexAddress.

Utilice el siguiente comando de RACADM para verificar la tarjeta de función SD y el estado de esta:

```
racadm featurecard -s
```

Tabla 6-1. 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 insertó correctamente. En una configuración de CMC redundante, 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.
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, tarjeta SD SN = 01122334455	Quite la tarjeta SD; localice e instale la tarjeta SD del 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 <code>racadm racreset</code> hasta que el módulo del CMC con la tarjeta de función instalada se active.

Utilice el siguiente comando `RACADM` para mostrar todas las funciones activadas en el chasis:

```
racadm feature -s
```

El comando produce el mensaje de estado siguiente:

```
Función = FlexAddress
```

```
Fecha de activación = 8 April 2008 - 10:39:40
```

```
Función instalada desde la tarjeta SD SN = 01122334455
```

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

```
racadm feature -s
```

```
No hay funciones activadas en el chasis.
```

Las tarjetas de función de Dell pueden contener más de una función. Cuando cualquiera de las funciones incluidas en una tarjeta de función de Dell se ha activado en el chasis, las demás funciones incluidas en la tarjeta no podrán activarse en otro chasis. En este caso, el comando `racadm feature -s` muestra el siguiente mensaje para las funciones afectadas:

```
ERROR: Una o más funciones de la tarjeta SD se encuentran activas en otro chasis.
```

Para obtener más información sobre los comandos RACADM, consulte las secciones de los comandos **feature** y **featurecard** de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Desactivación de FlexAddress

La función FlexAddress se puede desactivar y la tarjeta SD se puede regresar a un estado previo a la instalación a través de un comando de RACADM.

No hay ninguna función de desactivación en la interfaz web. La desactivación regresa la tarjeta SD a su estado original, en el cual se puede instalar y activar en un chasis diferente.



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 a la tarjeta.

Desactivación de FlexAddress

Utilice el siguiente comando de RACADM para desactivar la función FlexAddress y restaurar la tarjeta SD:

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

El comando mostrará el siguiente mensaje de estado tras la desactivación satisfactoria:

```
La función FlexAddress se ha desactivado 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: 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 la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Configuración de FlexAddress a través de la CLI



NOTA: Debe activar tanto la ranura como la red Fabric para que la dirección MAC asignada por el chasis sea enviada al iDRAC.



NOTA: También puede ver el estado de FlexAddress a través de la interfaz gráfica del usuario. Para obtener más información, consulte "FlexAddress" en la página 243.

Puede utilizar la interfaz de línea de comandos para activar o desactivar FlexAddress por cada red Fabric. Además, puede activar/desactivar la función por ranura. Después de haber activado la función por red Fabric, puede seleccionar las ranuras que se activarán. Por ejemplo, si solamente la red Fabric A está activada, todas las ranuras que estén activadas tendrán FlexAddress activado solo en la red Fabric A. El resto de las redes Fabric utilizarán la WWN/MAC asignada de fábrica en el servidor. Para que esta función funcione, la red Fabric debe estar activada y el servidor debe estar apagado.

Las ranuras activadas tendrán FlexAddress activado para todas las redes Fabric activadas. Por ejemplo, no es posible activar la red Fabric A y B y tener la ranura 1 con FlexAddress activado en la red Fabric A pero no en la red Fabric B.

Utilice el siguiente comando de RACADM para activar o desactivar redes Fabric:

```
racadm setflexaddr [-f <nombre_de_red_Fabric> <estado>]
```

<nombre_de_red_Fabric> = A, B, C, or iDRAC

<estado> = 0 or 1

Donde 0 es desactivar y 1 es activar.

Utilice el siguiente comando de RACADM para activar o desactivar ranuras:

```
racadm setflexaddr [-i <n.º de ranura> <estado>]
```

<n.º de ranura> = 1 to 16

<estado> = 0 or 1

Donde 0 es desactivar y 1 es activar.

Para obtener más información sobre el comando, consulte la sección del comando **feature** de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

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 de configuración adicionales:

- 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 le presenta el menú de detección de hardware, que detecta el cambio en la dirección MAC ya que se quitó y agregó hardware.

Cómo ver el estado de FlexAddress a través de la CLI

Puede utilizar la interfaz de línea de comandos para ver información del estado de FlexAddress. Puede ver información del estado del chasis completo o de una ranura específica. La información que se muestra incluye:

- Configuración de la red Fabric
- FlexAddress activado/desactivado
- Número y nombre de la ranura
- Direcciones asignadas por el chasis y por el servidor
- Direcciones en uso

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 <n.º de ranura>]
```

```
<n.º de ranura> = 1 to 16
```

Ver “Configuración de FlexAddress a través de la CLI” en la página 263 para obtener detalles adicionales sobre la configuración de FlexAddress. Para obtener más información sobre el comando, consulte la sección del comando **getflexaddr** de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Configuración de FlexAddress a través de la interfaz gráfica de usuario

Encendido en LAN con FlexAddress

Cuando se instala 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).

Solución de problemas de FlexAddress

Esta sección contiene información de solución de problemas para FlexAddress.

1 ¿Qué sucede si se quita una tarjeta de función?

No pasa nada. Las tarjetas de función se pueden quitar y almacenar o se pueden dejar colocadas.

2 ¿Qué sucede si se quita una tarjeta de función que se utilizó en un chasis y se coloca en otro?

La interfaz web mostrará un error que dice:

Esta tarjeta de función fue activada con otro chasis. Debe quitarse antes de acceder a la función FlexAddress.

Etiqueta de servicio del chasis actual = XXXXXXXXX

Etiqueta de servicio del chasis de la tarjeta de función = YYYYYYYY

Se agregará una anotación al registro del CMC que indica:

```
cmc <fecha de marca de tiempo timestamp> : función "FlexAddress@YYYYYYY" no activada; identificación del chasis='XXXXXXXX'
```

- 3** ¿Qué sucede si se quita la tarjeta de función y se instala una tarjeta que no sea de FlexAddress?

La tarjeta no deberá activarse ni sufrir modificaciones. El CMC ignora la tarjeta. En esta situación, el comando `$racadm featurecard -s` mostrará el mensaje:

```
No se insertó ninguna tarjeta de función
```

```
ERROR: No se puede abrir el archivo
```

- 4** 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 chasis o cualquier otro, la interfaz web mostrará el siguiente error:

```
Esta tarjeta de función fue activada con otro chasis. Debe quitarse antes de acceder a la función FlexAddress.
```

```
Etiqueta de servicio del chasis actual =  
XXXXXXXXXX
```

```
Etiqueta de servicio del chasis de la tarjeta  
de función = YYYYYYYYY
```

La tarjeta de función original ya no se puede seleccionar para desactivarla en ese chasis ni en ningún otro, salvo que el servicio de Dell vuelva a programar la etiqueta de servicio del chasis original en un chasis y que el CMC con la tarjeta de función original se active en ese chasis.

- La función FlexAddress se mantiene activa en el chasis vinculado original. La función de *vinculación de ese chasis* se actualiza para mostrar la nueva etiqueta de servicio.

- 5** ¿Se produce un error si tengo dos tarjetas de función instaladas en mi sistema CMC redundante?

La tarjeta de función en el CMC activo estará activada e instalada en el chasis. El CMC ignora la segunda tarjeta.

6 ¿La tarjeta SD tiene un dispositivo de protección contra escritura?

Sí. Antes de instalar la tarjeta SD en el módulo CMC, verifique que el pestillo de protección contra escritura esté en la posición desbloqueada. No se puede activar la función FlexAddress si la tarjeta SD está protegida contra escritura. En esta situación, el comando `$racadm feature -s` mostrará este mensaje:

```
No hay funciones activadas en el chasis. ERROR:  
Sistema de archivos de solo lectura
```

7 ¿Qué sucede si no hay una tarjeta SD en el módulo CMC activo?

El comando `$racadm featurecard -s` mostrará este mensaje:

```
No se insertó ninguna tarjeta de función.
```

8 ¿Qué le sucederá 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 antes de que pueda utilizarse con FlexAddress. Después de que se complete la actualización del BIOS del servidor, el módulo del servidor no obtendrá direcciones asignadas por el chasis hasta que se realice un ciclo de encendido en el servidor.

9 ¿Qué sucede si un chasis con un solo CMC se degrada para instalar un firmware anterior a la versión 1.10?

- La función y configuración de FlexAddress se desinstalarán del chasis.
- La tarjeta de función que se utiliza para activar la función en este chasis no cambia y se mantiene vinculada al chasis. Cuando el firmware del CMC del chasis se actualiza posteriormente a la versión 1.10 o superior, la función FlexAddress se reactiva al reinsertar la tarjeta de función original (si es necesario), restablecer el CMC (si la tarjeta de función se insertó después de completar la actualización de firmware) y reconfigurar la función.

- 10** ¿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 que tiene firmware inferior a 1.10, se debe seguir el siguiente procedimiento para asegurarse que NO se elimine la configuración y la función de FlexAddress actual.

- a** Asegúrese de que la versión del firmware del CMC activo sea siempre 1.10 o superior.
- b** Quite el CMC en espera e inserte el nuevo CMC en su lugar.
- c** 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 se produce una protección contra fallas, la función FlexAddress no se configurará y se deberá reactivar y reconfigurar la función.

- 11** La tarjeta SD no se encontraba en el chasis cuando ejecuté el comando de desactivación en FlexAddress. ¿Cómo recupero ahora mi tarjeta SD?

El problema es que la tarjeta SD no se puede utilizar para instalar FlexAddress en otro chasis si no estaba en el CMC cuando se desactivó FlexAddress. Para recuperar el uso de la tarjeta, vuelva a insertarla en el CMC del chasis al que está vinculada, reinstale FlexAddress y vuelva a desactivar FlexAddress.

- 12** Tengo la tarjeta SD instalada correctamente al igual que todas las actualizaciones de firmware/software. Veo que FlexAddress está activado, pero no puedo ver nada en la pantalla de implementación del servidor para implementarlo. ¿Cuál es el problema?

Éste es un problema de almacenamiento en caché del explorador; cierre el explorador y vuelva a abrirlo.

- 13** ¿Qué sucede con FlexAddress si debo restablecer la configuración del chasis con el comando RACADM, `racresetcfg`?

La función FlexAddress seguirá activada y lista para utilizarse. De forma predeterminada, se seleccionarán todas las redes Fabric y las ranuras.



NOTA: Se recomienda especialmente apagar el chasis antes de ejecutar el comando RACADM `racresetcfg`.

Mensajes de comandos

La siguiente tabla muestra los comandos RACADM y los mensajes de situaciones comunes de FlexAddress.

Tabla 6-2. Comandos y mensajes de salida de FlexAddress

Situación	Comando	Salida
La tarjeta SD en el módulo CMC activo está vinculada a otra etiqueta de servicio.	<code>\$racadm featurecard -s</code>	La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: la tarjeta de función está vinculada a otro chasis, svctag = <número de etiqueta de servicio> SN de tarjeta SD =<número de serie válido de la dirección flexible>
La tarjeta SD en el módulo CMC activo está vinculada a la misma etiqueta de servicio.	<code>\$racadm featurecard -s</code>	La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: La tarjeta de función está vinculada a este chasis

Tabla 6-2. Comandos y mensajes de salida de FlexAddress (continuación)

Situación	Comando	Salida
La tarjeta SD en el módulo CMC activo no está vinculada a ninguna etiqueta de servicio.	<code>\$racadm featurecard -s</code>	La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: La tarjeta de función no está vinculada a ningún chasis
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)	<code>\$racadm setflexaddr [-f <fabricName> <slotState>] OR \$racadm setflexaddr [-i <slot#> <slotState>]</code>	ERROR: La función Flexaddress no está activada en el chasis
El usuario invitado intenta configurar FlexAddress en ranuras/redes Fabric	<code>\$racadm setflexaddr [-f <fabricName> <slotState>] \$racadm setflexaddr [-i <slot#> <slotState>]</code>	ERROR: Privilegios de usuario insuficientes para realizar la operación
Desactivar la función FlexAddress con el chasis encendido.	<code>\$racadm feature -d -c flexaddress</code>	ERROR: No se puede desactivar la función porque el chasis está encendido
El usuario invitado intenta desactivar la función en el chasis.	<code>\$racadm feature -d -c flexaddress</code>	ERROR: Privilegios de usuario insuficientes para realizar la operación

Tabla 6-2. Comandos y mensajes de salida de FlexAddress (continuación)

Situación	Comando	Salida
Cambiar la configuración de FlexAddress de ranuras/redes Fabric mientras los módulos del servidor están encendidos.	<code>\$racadm setflexaddr -i 1 1</code>	ERROR: No se puede realizar la operación de establecimiento porque afecta a un servidor encendido
¿Por qué falla el comando <code>racadm setflexaddr</code> en el CMC (aún activo) después de desactivar únicamente la función FlexAddressPlus (dejando activado FlexAddress)?		Si el CMC pasa a estar activo posteriormente, con la tarjeta de función FlexAddressPlus insertada en la ranura, la función FlexAddressPlus se reactiva y se pueden reanudar los cambios de la configuración de FlexAddress para ranuras y redes Fabric.

CONTRATO DE LICENCIA DEL 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 su 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 integrado 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 será “utilizarlo” siempre y cuando usted disponga de una licencia independiente para cada equipo al que se haya distribuido el Software. Debe asegurarse de que el número de personas que utilicen el Software instalado en un servidor de red no sea superior al número de licencias de las que disponga. Si el número de usuarios del Software instalado en un servidor de red supera el número de licencias, deberá adquirir licencias adicionales hasta que tenga el mismo número de licencias que de usuarios, antes de 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 usted hace del Software. La auditoría se limitará a la verificación del cumplimiento de los términos de este contrato por su parte.

El Software está protegido por las leyes de derechos de autor de Estados Unidos y por tratados internacionales. 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 el software ni copiar los materiales impresos que se adjuntan con el mismo, 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 pulgadas o de 5,25 pulgadas, 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 permite 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 un accidente, abuso, aplicación indebida, mantenimiento o modificación 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 usted 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 haya finalizado, usted acepta que procederá a la destrucción del Software y 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 un 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.

Preguntas frecuentes

En la Tabla 6-3 se enumeran las preguntas más frecuentes sobre la función FlexaddressPlus.

Tabla 6-3. FlexaddressPlus

Pregunta	Respuesta
Después de desactivar únicamente la función FlexAddressPlus (dejando activado FlexAddress), ¿por qué falla el comando <code>racadm set flexaddr</code> en el CMC (aún activo)?	Si el CMC pasa a estar activo posteriormente, con la tarjeta de función FlexAddressPlus insertada en la ranura, la función FlexAddressPlus se reactiva y se pueden reanudar los cambios de la configuración de FlexAddress para ranuras y redes Fabric.

Uso de FlexAddress Plus

FlexAddress Plus es una nueva función que se ha añadido 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 FlexAddress Plus contiene más direcciones MAC que la función FlexAddress. Ambas funciones le permiten al chasis asignar direcciones WWN/MAC (Nombre a nivel 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.

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 como FlexAddress solo contiene FlexAddress, y la tarjeta etiquetada como FlexAddress Plus contiene FlexAddress y FlexAddress Plus. Debe insertarse esta tarjeta en la CMC para activar la función.

Según la configuración, es posible que algunos servidores, como el PowerEdge M710HD, requieran más direcciones MAC de las que FA puede proporcionar al CMC. Para estos servidores, la actualización a FlexAddress Plus permitirá optimizar por completo la configuración de direcciones WWN/MAC. Para obtener asistencia en relación con la función FlexAddress Plus, comuníquese con Dell.

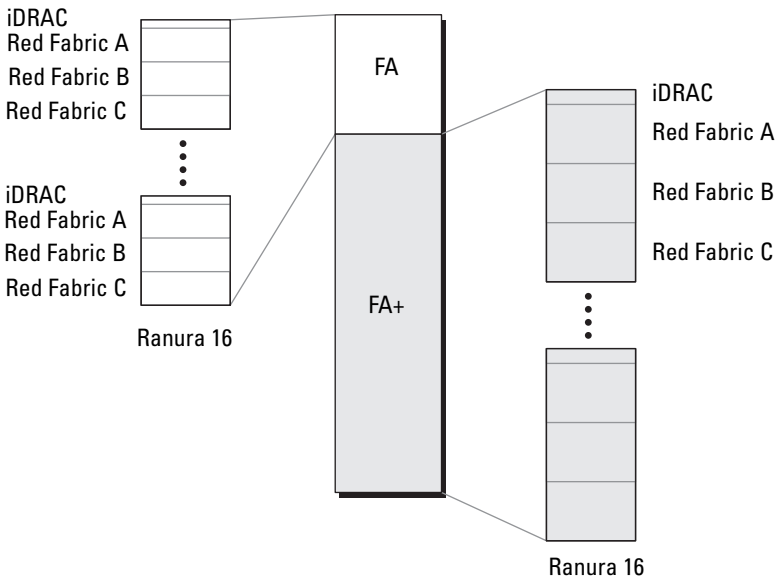
Para activar la función FlexAddress Plus se requieren las siguientes actualizaciones de software: BIOS del servidor, iDRAC del servidor y firmware de CMC. Si estas actualizaciones no se aplican, solo estará disponible la función FlexAddress. Para obtener más información acerca de las versiones mínimas necesarias de estos componentes, consulte el archivo Léame de CMC 4.0 en el sitio support/dell.com/manuals.

Comparación de 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. La tabla que aparece a continuación 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 7-1. Funciones de FlexAddress (FA) y FlexAddress Plus (FA+)



Uso del servicio de directorio del CMC

Un servicio de directorio mantiene una base de datos común con toda la información necesaria para controlar los usuarios, equipos, impresoras y demás componentes de la red. Si su empresa utiliza el software Microsoft Active Directory o el software de servicio de directorios LDAP, puede configurar el CMC para utilizar la autenticación de usuarios basada en directorios.

Uso del CMC con Microsoft Active Directory



NOTA: El uso de Active Directory para reconocer a los usuarios del CMC se admite en los sistemas operativos Microsoft Windows 2000 y Windows Server 2003. Active Directory con IPv6 e IPv4 solo se admite en Windows 2008.

Extensiones de esquema de Active Directory

Puede utilizar Active Directory para definir el acceso de los usuarios al CMC mediante dos métodos:

- La solución de esquema estándar, que utiliza solo los objetos de grupo estándares de Active Directory.
- La solución de esquema extendido, que utiliza objetos de Active Directory definidos por Dell.

Esquema estándar y esquema extendido

Cuando se utiliza Active Directory para configurar el acceso al CMC, se debe elegir la solución de esquema extendido o de esquema estándar.

Con la solución de esquema estándar:

- No se requiere la extensión del esquema porque el esquema estándar utiliza únicamente objetos estándares de Active Directory.
- La configuración de Active Directory es sencilla.

Con la solución de esquema extendido:

- Todos los objetos de control de acceso se mantienen en Active Directory.
- La configuración del acceso de los usuarios en distintos CMC y con distintos niveles de privilegios proporciona la máxima flexibilidad.

Generalidades del esquema estándar de Active Directory

El uso del esquema estándar para la integración de Active Directory requiere tareas de configuración en Active Directory y el CMC.

En Active Directory se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso al CMC es miembro del grupo de funciones.

Para que este usuario tenga acceso a una tarjeta de CMC específica, es necesario configurar el nombre del grupo de funciones y su nombre de dominio en dicha tarjeta de CMC. A diferencia del esquema extendido, la función y el nivel de privilegios se definen en cada tarjeta de CMC y no en Active Directory. En cada CMC pueden configurarse y definirse hasta cinco grupos de funciones. Ilustración 8-1 muestra la configuración del CMC con Active Directory y esquema estándar La Tabla 5-43 muestra el nivel de privilegios de los grupos de funciones y la Tabla 8-1 muestra la configuración predeterminada del grupo de funciones.

Ilustración 8-1. Configuración del CMC con Active Directory y esquema estándar

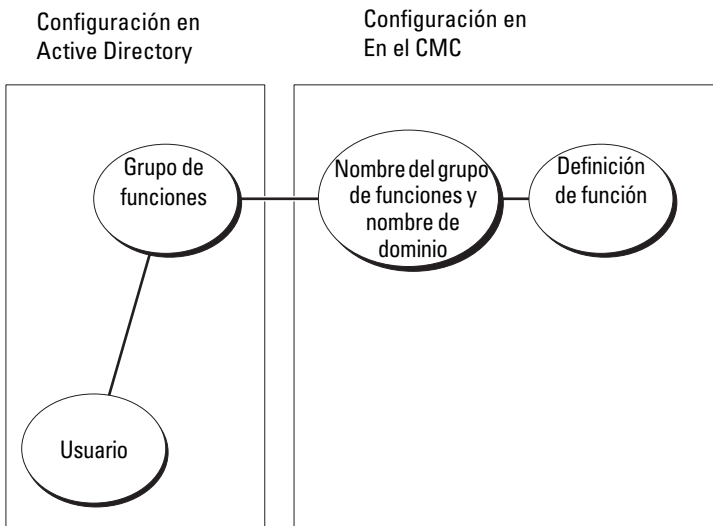


Tabla 8-1. Privilegios predeterminados del grupo de funciones

Grupo de funciones	Privilegio predeterminado Nivel	Permisos otorgados	Máscara de bits
1	Ninguno	<ul style="list-style-type: none">• 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• Superusuario• 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	0x00000fff
2	Ninguno	<ul style="list-style-type: none">• Usuario con acceso al CMC• Administrador de borrado de registros• Administrador de control del chasis• 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 usuarios, ver “Tipos de usuarios” en la página 173.

Hay dos maneras de activar el esquema estándar de Active Directory:

- Por medio de la interfaz web del CMC. Vea la “Configuración del CMC con Active Directory de esquema convencional y la interfaz web” en la página 284.
- Con la herramienta de CLI de RACADM. Vea la “Configuración del CMC con Active Directory de esquema convencional y RACADM” en la página 287.

Configuración de Active Directory con esquema estándar para acceder al CMC

Para que un usuario de Active Directory pueda acceder al CMC, realice los pasos que se indican a continuación para configurar Active Directory:

- 1 En un servidor de Active Directory (controladorA de dominio), abra el complemento de usuarios y equipos de Active Directory.
- 2 Cree un grupo o seleccione un grupo existente. El nombre del grupo y el nombre de este dominio se deben configurar en el CMC por medio de la interfaz web o con RACADM.

Para obtener más información, ver “Configuración del CMC con Active Directory de esquema convencional y la interfaz web” en la página 284 o “Configuración del CMC con Active Directory de esquema convencional y RACADM” en la página 287.

- 3 Agregue el usuario de Active Directory como miembro del grupo de Active Directory para acceder al CMC.

Configuración del CMC con Active Directory de esquema convencional y la interfaz web

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Chasis** en el árbol del sistema.
- 3 Haga clic en **Autenticación de usuarios**→ **Servicios de directorios**. Aparecerá la página **Servicios de directorios**.

4 Seleccione el botón de radio que se encuentra junto a la opción Microsoft Active Directory (esquema estándar). Aparecerá la página **Configuración y administración de Active Directory**.

5 En la sección **Valores comunes**:

a Seleccione la casilla de verificación **Habilitar Active Directory**.

b Escriba el **Nombre del dominio raíz**.



NOTA: El **Nombre de dominio raíz** debe ser un nombre de dominio válido que siga la convención para la asignación de nombres *x.y*, donde *x* es una cadena de 1 a 256 caracteres ASCII sin espacios entre los caracteres, mientras que *y* es un tipo de dominio válido como *com*, *edu*, *gov*, *int*, *mil*, *net* u *org*.

c Escriba el **Tiempo de espera** en segundos. El rango del tiempo de espera es de 15 a 300 segundos. El tiempo de espera predeterminado es de 90 segundos.

6 Si desea que la ejecución dirigida realice una búsqueda en la controladora de dominio y el catálogo global, seleccione la casilla de verificación **Buscar servidor de AD para la búsqueda (opcional)** y después realice el siguiente procedimiento:

a En el campo de texto **Controladora de dominio**, escriba el servidor en el que está instalado el servicio Active Directory.

b En el campo de texto **Catálogo global**, escriba la ubicación del catálogo global en la controladora de dominio de Active Directory. El catálogo global ofrece un recurso para buscar un bosque de Active Directory.

7 Haga clic en **Aplicar** para guardar la configuración.



NOTA: Debe aplicar la configuración antes de continuar con el siguiente paso. De lo contrario, la configuración que ingresó se perderá cuando avance a la siguiente página.

8 En la sección **Configuración del esquema estándar**, haga clic en un **Grupo de funciones**. Aparece la página **Configurar grupo de funciones**.

9 Escriba el **Nombre de grupo**. El nombre de grupo identifica el grupo de funciones en el servicio Active Directory relacionado con la tarjeta del CMC.

10 Escriba el **Dominio del grupo**. El **Nombre de grupo** es el nombre del dominio raíz completamente expresado para el bosque.

- 11 En la página **Privilegios del grupo de funciones**, seleccione los privilegios del grupo.

Si modifica alguno de los privilegios, el **Privilegio del grupo de funciones** ya existente (administrador, usuario avanzado o usuario invitado) cambiará al grupo personalizado o al privilegio de grupo de funciones que corresponda. Vea la Tabla 5-43.

- 12 Haga clic en **Aplicar** para guardar la configuración del grupo de funciones.
- 13 Haga clic en la página **Volver a configuración**.
- 14 Cargue el certificado con la firma de la autoridad de certificados raíz de bosque de dominio en el CMC. En la sección **Administración de certificados**, escriba la ruta de acceso del certificado o diríjase al directorio del archivo del certificado. Haga clic en el botón **Cargar** para transferir el archivo al CMC.



NOTA: El valor **Ruta de acceso del archivo** muestra la ruta de acceso relativa del archivo del certificado que se va a cargar. Debe escribir la ruta de acceso absoluta al archivo, 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.

- 15 Haga clic en **Aplicar**. El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.
- 16 Cierre sesión y luego inicie sesión en el CMC para completar la configuración de la función de Active Directory del CMC.
- 17 Seleccione **Chasis** en el árbol del sistema.
- 18 Haga clic en la ficha **Red**.
- 19 Haga clic en la subficha **Red**. Aparecerá la página **Configuración de la red**.

- 20** Si la opción **Usar DHCP** (para la dirección IP de la interfaz de red del CMC) está seleccionada en **Configuración de la red**, seleccione **Usar DHCP para obtener la dirección del servidor DNS**.

Para introducir manualmente una dirección IP del servidor DNS, deje en blanco la opción **Usar DHCP para obtener las direcciones de servidor DNS** y escriba las direcciones IP del servidor DNS principal y alternativo.

- 21** Haga clic en **Aplicar cambios**.

Se ha completado la configuración de la función de Active Directory de esquema estándar del CMC.

Configuración del CMC con Active Directory de esquema convencional y RACADM

Para configurar el componente Active Directory del CMC con esquema estándar por medio de la CLI de RACADM, utilice los siguientes comandos:

- 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 del dominio raíz
completamente expresado>
racadm config -g cfgStandardSchema -i <índice> -o
cfgSSADRoleGroupName <nombre común del grupo de
funciones>
racadm config -g cfgStandardSchema -i <índice> -o
cfgSSADRoleGroupDomain <nombre de dominio
completamente expresado>
racadm config -g cfgStandardSchema -i <índice> -o
cfgSSADRoleGroupPrivilege <número de la máscara de
bits para los permisos del usuario específico>
racadm sslcertupload -t 0x2 -f <certificado CA
raíz de ADS>
racadm sslcertdownload -t 0x1 -f <certificado raíz
SSL de RAC>
```



NOTA: Para ver los valores del número de la máscara de bits, consulte la tabla 3-1 en el capítulo de propiedades de la base de datos de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 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 por 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 del DNS primario>
```

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

Descripción general del esquema extendido

Hay dos maneras de activar el esquema extendido de Active Directory:

- Mediante el uso de la interfaz web del CMC. Para obtener instrucciones, ver “Configuración del CMC con Active Directory de esquema extendido y la interfaz web” en la página 305.
- Mediante el uso de la herramienta de CLI de RACADM. Para obtener instrucciones, ver “Configuración del CMC con Active Directory de esquema extendido y RACADM” en la página 309.

Extensiones de esquema de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos.

Un ejemplo de las clases almacenadas en la base de datos es la clase usuario. Los atributos de esta clase pueden incluir el nombre, apellido, número de teléfono y otros datos del usuario.

La base de datos de Active Directory puede ampliarse mediante la incorporación de atributos y clases propios y exclusivos que respondan a las necesidades específicas del entorno de su empresa. Dell ha extendido el esquema para incluir los cambios necesarios para admitir la autenticación y autorización de administración remota.

Cada atributo o clase que se agrega a un esquema existente de Active Directory debe ser definido con una identificación única. Para conservar la exclusividad de las identificaciones en toda la industria, Microsoft mantiene una base de datos de identificadores de objetos (OID) de Active Directory. Para ampliar el esquema de Active Directory, Dell estableció identificadores de objetos únicos, extensiones de nombre únicas e identificaciones de atributos vinculadas de manera exclusiva para los atributos y clases específicos de Dell:

Extensión de Dell: dell

OID base de Dell: 1.2.840.113556.1.8000.1280

Rango de identificaciones vinculadas del RAC: 12070–2079

Descripción general de las extensiones de esquema de RAC

Dell proporciona un grupo de propiedades que pueden configurarse. El esquema extendido de Dell incluye propiedades de asociación, dispositivos y privilegios.

La propiedad de asociación vincula a usuarios o grupos con un conjunto específico de privilegios con uno o más dispositivos de RAC. Este modelo proporciona al administrador la máxima flexibilidad sobre las combinaciones diferentes de usuarios, privilegios de RAC y dispositivos de RAC en la red sin agregar demasiada complejidad.

Descripción general de los objetos de Active Directory

Si existen dos CMC en la red que se desean integrar a Active Directory para fines de autenticación y autorización, será necesario crear al menos un objeto de asociación y un objeto de dispositivo de RAC para cada CMC. Puede crear varios objetos de asociación y cada objeto de asociación puede ser vinculado a cuantos usuarios, grupos de usuarios u objetos del dispositivo del 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 solo un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en los CMC específicos.

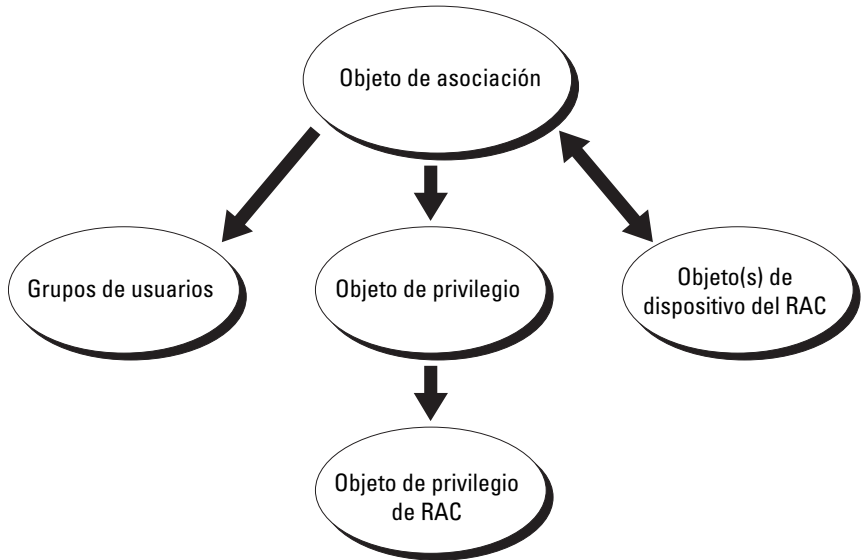
El objeto del dispositivo del RAC es el vínculo con el firmware de RAC para consultar a Active Directory para fines de autenticación y autorización. Cuando se agrega un RAC a la red, el administrador debe configurar el RAC y su objeto de dispositivo con el nombre de Active Directory, de modo que los usuarios puedan realizar la autenticación y la autorización con Active Directory. Además, el administrador también debe agregar el RAC a por lo menos un objeto de asociación para que los usuarios se puedan autenticar. La Ilustración 8-2 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autenticaciones y autorizaciones.



NOTA: El objeto de privilegio de RAC se aplica al DRAC 4, el DRAC 5 y el CMC.

Pueden crearse tantos objetos de asociación como sea necesario. No obstante, es necesario crear al menos un objeto de asociación y disponer de un objeto del dispositivo del RAC para cada RAC (CMC) de la red que se desee integrar a Active Directory.

Ilustración 8-2. Configuración típica de los objetos de Active Directory

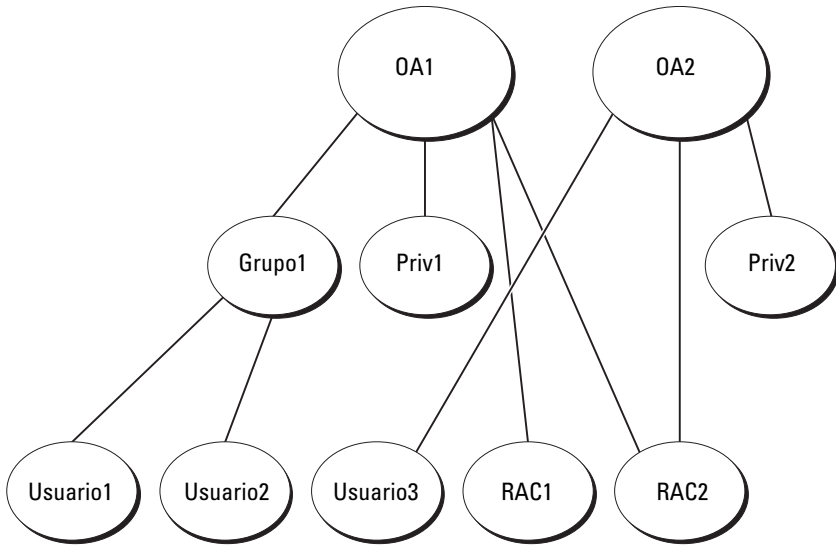


El objeto de asociación permite tener la cantidad de usuarios y/o grupos así como los objetos de dispositivo de RAC. Sin embargo, el objeto de asociación solo incluye un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los “usuarios” que tienen “privilegios” en los RAC (CMC).

Además, se pueden configurar objetos de Active Directory en un solo dominio o en varios. Por ejemplo, supongamos que tiene dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory (usuario1, usuario2 y usuario3). Usted desea otorgar privilegios de administrador para ambos CMC a los usuarios 1 y 2, y privilegios de inicio de sesión en la tarjeta de RAC2 para el usuario3. La Ilustración 8-3 muestra cómo configurar los objetos de Active Directory en esta situación.

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

Ilustración 8-3. Configuración de objetos de Active Directory en un solo dominio



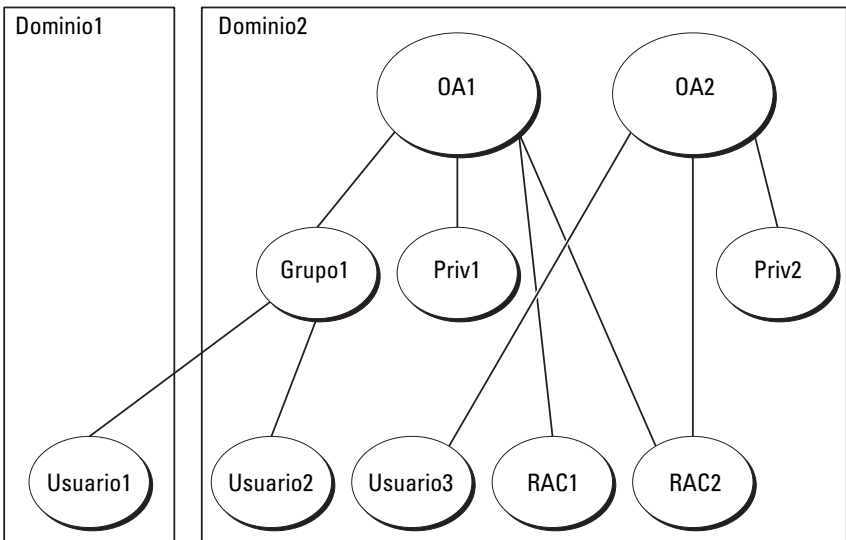
Cómo configurar los objetos para un solo dominio:

- 1 Cree dos objetos de asociación.
- 2 Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representarán a los dos CMC.
- 3 Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (de administrador) y Priv2 tiene privilegio de inicio de sesión.
- 4 Agrupe usuario1 y usuario2 en el Grupo1.
- 5 Agregue el 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 el 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.

Para obtener instrucciones detalladas, ver “Cómo agregar usuarios y privilegios del CMC a Active Directory” en la página 302.

La Ilustración 8-4 muestra un ejemplo de los objetos de Active Directory en varios dominios. En esta situación, existen dos CMC (RAC1 y RAC2) y tres usuarios de Active Directory (usuario1, usuario2 y usuario3). El usuario1 está en el Dominio1, y el usuario2 y el usuario 3 están en el Dominio2. En esta situación, 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.

Ilustración 8-4. Configuración de objetos de Active Directory en varios dominios



Para configurar los objetos para 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.

La Ilustración 8-4 muestra los objetos en el Dominio2.

- 3 Cree dos objetos de dispositivo del RAC, RAC1 y RAC2, que representarán a los dos CMC.
- 4 Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tiene todos los privilegios (de administrador) y Priv2 tiene privilegio de inicio de sesión.
- 5 Agrupe usuario1 y usuario2 en el Grupo1. El ámbito de grupo del Grupo1 debe ser Universal.
- 6 Agregue el 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.
- 7 Agregue el 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.

Configuración de Active Directory con esquema extendido para acceder al CMC

Antes de utilizar Active Directory para acceder al CMC, debe configurar el software Active Directory y el CMC:

- 1 Extienda el esquema de Active Directory (ver “Cómo extender el esquema de Active Directory” en la página 295).
- 2 Extienda el complemento Usuarios y equipos de Active Directory (ver “Instalación de la extensión de Dell para el complemento Usuarios y equipos de Active Directory” en la página 301).
- 3 Agregue usuarios de CMC y sus privilegios a Active Directory (ver “Cómo agregar usuarios y privilegios del CMC a Active Directory” en la página 302).
- 4 Active SSL en cada uno de las controladoras de dominio.
- 5 Configure las propiedades de Active Directory de CMC por medio de la interfaz web del CMC o la RACADM (ver “Configuración del CMC con Active Directory de esquema extendido y la interfaz web” en la página 305 o “Configuración del CMC con Active Directory de esquema extendido y RACADM” en la página 309).

Cómo extender el esquema de Active Directory

La extensión del esquema de Active Directory agrega una unidad organizacional Dell, clases y atributos de esquema, así como privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender el esquema, asegúrese de contar con privilegios de administrador de esquema en el dueño de las funciones de operaciones de maestro único flexible (FSMO) de maestro de esquema del bosque de dominio.

Puede extender el esquema por medio de uno de los siguientes métodos:

- Utilidad Dell Schema Extender
- Archivo de secuencia de comandos LDIF

Si utiliza el archivo de secuencia de comandos LDIF, la unidad organizacional de Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell System Management) en los siguientes directorios respectivamente:

- <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools<tipo de instalación>\LDIF Files
- <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools<tipo de instalación>\Schema Extender

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que se incluye en el directorio **LDIF_Files**. Para obtener instrucciones sobre el uso de Dell Schema Extender para extender el esquema de Active Directory, ver “Uso de Dell Schema Extender” en la página 295.

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 garantizar que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

- 1 En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
- 2 Lea y comprenda la advertencia y haga clic en **Siguiente**.

- 3 Seleccione **Usar las credenciales de inicio de sesión actuales** o introduzca un nombre de usuario y una contraseña con derechos de administrador de esquema.
- 4 Haga clic en **Siguiente** para ejecutar Dell Schema Extender.
- 5 Haga clic en **Terminar**.

El esquema ha sido extendido. Para verificar la extensión del esquema, utilice la Consola de administración de Microsoft (MMC) y el complemento Esquema de Active Directory para verificar que existan los siguientes elementos:

- Clases: ver de la Tabla 8-2 a la Tabla 8-7.
- Atributos: ver la Tabla 8-8

Consulte la documentación de Microsoft para obtener más información acerca de cómo activar y utilizar el complemento Esquema de Active Directory en MMC.

Tabla 8-2. Definiciones de las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	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 8-3. Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Descripción	Representa el dispositivo RAC de Dell. El dispositivo RAC debe estar configurado como dellRacDevice en Active Directory. Esta configuración permite que el CMC envíe consultas de Protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
Superclases	dellProduct
Atributos	dellSchemaVersion dellRacType

Tabla 8-4. Clase dellAssociationObject

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
Superclases	Grupo
Atributos	dellProductMembers dellPrivilegeMember

Tabla 8-5. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los derechos de autorización (privilegios) del dispositivo CMC.
Tipo de clase	Clase auxiliar
Superclases	Ninguno
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tabla 8-6. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Clase que contiene los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
Superclases	Usuario
Atributos	dellRAC4Privileges

Tabla 8-7. Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
Superclases	Computadora
Atributos	dellAssociationMembers

Tabla 8-8. 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 los objetos de dellPrivilege que pertenecen a este atributo.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.1	FALSO
Nombre distintivo: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Atributo: dellProductMembers	
Descripción: lista de los objetos de dellRacDevices que pertenecen a esta función. Este atributo es el vínculo para avanzar al vínculo dellAssociationMembers.	
Identificación de vínculo: 12070	
OID: 1.2.840.113556.1.8000.1280.1.1.2.2	FALSO
Nombre distintivo: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	

Tabla 8-8. Lista de atributos agregados al esquema de Active Directory (continuación)

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
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	VERDADERO
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Atributo: dellIsLoginUser	
Descripción: el valor es VERDADERO si el usuario tiene derechos de inicio de sesión en el dispositivo.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.3	VERDADERO
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	VERDADERO
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	VERDADERO
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Atributo: dellIsLogClearAdmin	
Descripción: el valor es VERDADERO si el usuario tiene derechos de administrador de borrado de registros en el dispositivo.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.6	VERDADERO
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

Tabla 8-8. Lista de atributos agregados al esquema de Active Directory (continuación)

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
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	VERDADERO
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	VERDADERO
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	VERDADERO
Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	VERDADERO
Cadena que no distingue entre mayúsculas y minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
Atributo: dellRacType	
Descripción: este atributo representa el tipo de RAC actual para el objeto dellRacDevice y el vínculo de retroceso del vínculo dellAssociationObjectMembers.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.13	VERDADERO
Cadena que no distingue entre mayúsculas y minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	

Tabla 8-8. Lista de atributos agregados al esquema de Active Directory (continuación)

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Atributo: dellAssociationMembers	
Descripción: lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso al atributo vinculado dellProductMembers.	
Identificación de vínculo: 12071	
OID: 1.2.840.113556.1.8000.1280.1.1.2.14	FALSO
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 la extensión de Dell 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), usuarios y grupos de usuarios, así como las asociaciones y los privilegios del RAC.

Cuando instala el software de administración de sistemas con el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) puede extender el complemento si selecciona la opción **Extensión de Dell para el complemento Usuarios y equipos de Active Directory** durante el procedimiento de instalación. Para obtener instrucciones adicionales sobre la instalación de software de administración de sistemas consulte la *Dell OpenManage Server Administrator Installation Guide* (Guía de instalación de Server Administrator de Dell OpenManage) y la *Dell OpenManage Management Station Software Installation Guide* (Guía de instalación de Management Station Software de OpenManage).

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

Instalación de Administrator Pack

Es necesario instalar Administrator Pack en cada sistema que administra los objetos del CMC de Active Directory. Si no instala Administrator Pack, no podrá ver el objeto RAC de Dell en el contenedor.

Cómo abrir el complemento Usuarios y equipos de Active Directory

Para abrir el complemento Usuarios y equipos de Active Directory:

- 1** Si está conectado en la controladora del dominio, haga clic en **Inicio**→ **Herramientas administrativas**→ **Usuarios y equipos de Active Directory**.
Si no está conectado en la controladora de dominio, debe tener el Microsoft Administrator Pack correspondiente instalado en el sistema local. Para instalar este Administrator Pack, haga clic en **Inicio**→ **Ejecutar**, escriba MMC y presione <Intro>. Aparecerá la ventana Consola de administración de Microsoft (MMC).
- 2** En la ventana **Consola 1**, haga clic en **Archivo** (o en **Consola**, en los sistemas que ejecutan Windows 2000).
- 3** Haga clic en **Agregar o quitar complemento**.
- 4** Seleccione el complemento **Usuarios y equipos de Active Directory** y haga clic en **Agregar**.
- 5** Haga clic en **Cerrar**.

Cómo agregar usuarios y privilegios del CMC a Active Directory

Con el complemento Usuarios y equipos de Active Directory extendido por Dell puede agregar usuarios y privilegios del CMC mediante la creación de objetos de RAC, de asociación y de privilegio. Para añadir cada tipo de objeto, haga lo siguiente:

- 1** Crear un objeto de dispositivo de RAC.
- 2** Crear un objeto de privilegio.
- 3** Crear un objeto de asociación.
- 4** Agregar objetos a un objeto de asociación.

Cómo crear un objeto de dispositivo de RAC

Para crear un objeto de dispositivo de RAC:

- 1** En la ventana **Raíz de consola** de MMC, haga clic con el botón derecho del mouse en un contenedor.
- 2** Seleccione **Nuevo**→ **Objeto de RAC de Dell**.
Aparece la ventana **Nuevo objeto**.
- 3** Escriba un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del CMC que escriba en paso a de “Configuración del CMC con Active Directory de esquema extendido y la interfaz web” en la página 305.
- 4** Seleccione **Objeto de dispositivo de RAC** y haga clic en **Aceptar**.

Cómo crear un objeto de privilegio



NOTA: Se debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

Para crear un objeto de privilegio:

- 1** En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
- 2** Seleccione **Nuevo**→ **Objeto de RAC de Dell**.
Aparece la ventana **Nuevo objeto**.
- 3** Escriba 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 del RAC** y seleccione los privilegios que desea otorgar al usuario. Para obtener más información sobre los privilegios de usuarios del CMC, ver “Tipos de usuarios” en la página 173.

Cómo crear un objeto de asociación

El objeto de asociación se deriva de un grupo y debe contener un tipo de grupo. El ámbito de la asociación especifica el tipo de grupo de seguridad para el objeto de asociación. Al crear un objeto de asociación, elija el ámbito de la asociación correspondiente al tipo de objetos que quiere agregar.

Por ejemplo, si selecciona **Universal** los objetos de asociación solo estarán disponibles cuando el dominio de Active Directory funcione en el modo nativo o superior. Para crear un objeto de asociación:

- 1 En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
- 2 Seleccione **Nuevo**→ **Objeto de RAC de Dell**.
Esto abrirá la ventana **Nuevo objeto**.
- 3 Escriba un nombre para el nuevo objeto.
- 4 Seleccione **Objeto de asociación**.
- 5 Seleccione el ámbito para el **Objeto de asociación** y haga clic en **Aceptar**.

Cómo agregar objetos a un objeto de asociación

Por medio de la ventana **Propiedades de objeto de asociación**, puede asociar a usuarios o grupos de usuarios, objetos de privilegio y dispositivos de RAC o grupos de dispositivos de RAC. Si el sistema ejecuta el modo Windows 2000 o posteriores, utilice los grupos universales para abarcar dominios con los objetos de RAC o usuario.

Puede agregar a grupos de usuario y dispositivos de RAC. El procedimiento para la creación de grupos relacionados con Dell y grupos ajenos a Dell es el mismo.

Cómo agregar usuarios o grupos de usuarios

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 Escriba el nombre del usuario o grupo de usuarios y haga clic en **Aceptar**.

Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios cuando se autentifican en un dispositivo RAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar privilegios

Para añadir privilegios:

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

Cómo 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 Escriba el nombre del dispositivo de RAC o del grupo de dispositivos de RAC y haga clic en **Aceptar**.
- 3 En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

Configuración del CMC con Active Directory de esquema extendido y la interfaz web

Para configurar el CMC con Active Directory de esquema extendido y la interfaz web:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Chasis** en el árbol del sistema.
- 3 Haga clic en **Autenticación de usuarios** → **Servicios de directorios**. Aparecerá la página **Servicios de directorios**.
- 4 Seleccione **Microsoft Active Directory (esquema extendido)**.
- 5 En la sección **Valores comunes**:
 - a Verifique que la casilla de verificación **Habilitar Active Directory** esté seleccionada.
 - b Escriba el **Nombre del dominio raíz**.



NOTA: El Nombre del dominio raíz debe ser un nombre de dominio válido expresado mediante la convención de nombres *x.y*, donde *x* es una cadena ASCII de 1 a 256 caracteres sin espacios intermedios, e *y* es un tipo de dominio válido como *com*, *edu*, *gov*, *int*, *mil*, *net* u *org*.

c Escriba el **Tiempo de espera** en segundos. **Rango de configuración:** De 15 a 300 segundos. **Valor predeterminado:** 90 segundos

6 **Opcional:** Si desea que la ejecución dirigida realice una búsqueda en la controladora de dominio y el catálogo global, seleccione la casilla de verificación **Buscar servidor de AD para la búsqueda (Opcional)** y luego haga lo siguiente:

a En el campo de texto **Controlador de dominio**, escriba el servidor en el que está instalado el servicio Active Directory.

b En el campo de texto **Catálogo global**, escriba la ubicación del catálogo global en la controladora de dominio de Active Directory. El catálogo global ofrece un recurso para buscar un bosque de Active Directory.



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



NOTA: Puede especificar una lista de servidores de controlador 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 controlador de dominio y de catálogo global que no han sido correctamente configurados para todos los dominios y aplicaciones pueden producir resultados inesperados durante el funcionamiento de las aplicaciones o dominios existentes.

7 En la sección **Configuración del esquema extendido:**


a Escriba el **Nombre del dispositivo de CMC**. El **Nombre del CMC** identifica de forma exclusiva la tarjeta del CMC en Active Directory. El **Nombre del CMC** debe ser igual al nombre común del nuevo objeto de CMC que se creó en la controladora de dominio. El **Nombre del CMC** debe ser una cadena de 1 a 256 caracteres ASCII sin espacios entre los caracteres.

- b Escriba el **Nombre de dominio del CMC** (ejemplo: `cmc.com`). El **Nombre de dominio del CMC** es el nombre DNS (cadena de caracteres) del dominio donde reside el objeto CMC de Active Directory. El nombre debe ser un nombre de dominio válido expresado como `x.y`, donde `x` es una cadena de 1 a 256 caracteres ASCII sin espacios entre ellos, `y` es un tipo de dominio válido, como `com`, `edu`, `gov`, `int`, `mil`, `net` u `org`.

8 Haga clic en **Aplicar** para guardar la configuración.

 **NOTA:** Antes de continuar en el paso siguiente, que permite acceder a otra página, debe aplicar la configuración. De lo contrario, se perderán los valores introducidos cuando acceda a la página siguiente.

9 En la sección **Administrar certificados**, escriba la ruta de archivo del certificado en el campo de texto o haga clic en **Examinar** para seleccionar el archivo del certificado. Haga clic en el botón **Cargar** para transferir el archivo al CMC.

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

La validación de certificados de SSL es obligatoria de forma predeterminada. Existe un nuevo parámetro de configuración en el grupo de RACADAM `cfgActiveDirectory` y en la interfaz gráfica de usuario para desactivar la comprobación de certificados.

 **PRECAUCIÓN:** Puede ser peligroso desactivar este certificado.

Para activar la validación de certificados de SSL (opción predeterminada):

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

Para desactivar la validación de certificados de SSL:

```
racadm config -g cfgActiveDirectory -o  
cfgADCertValidationEnable 0
```

Los certificados SSL para las controladoras de dominio deben estar firmados por 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.

- 10** Haga clic en **Aplicar**. El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.
- 11** Vuelva a iniciar sesión en la interfaz web del CMC.
- 12** 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**.
- 13** Si **Usar DHCP** para la dirección IP de la interfaz del CMC está activado, realice una de las siguientes operaciones:
 - 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 una dirección IP de servidor DNS: Deseleccione la casilla de verificación **Usar DHCP para obtener direcciones de servidor DNS** y luego escriba la direcciones IP de los servidores DNS primario y alternativo en los campos correspondientes.
- 14** Haga clic en **Aplicar cambios**.

Se ha completado la configuración del componente Active Directory de esquema extendido del CMC.

Configuración del CMC con Active Directory de esquema extendido y RACADM

Utilice los siguientes comandos para configurar el componente Active Directory del CMC con esquema extendido por medio de la herramienta de CLI de RACADM en lugar de utilizar la interfaz web.

- 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
cfgADRaDomain <nombre del dominio raíz
completamente expresado>
racadm config -g cfgActiveDirectory -o
cfgADRootDomain <nombre del dominio raíz
completamente expresado>
racadm config -g cfgActiveDirectory -o
cfgADRaName <nombre común de CMC>
racadm sslcertupload -t 0x2 -f <certificado de CA
de la raíz de ADS> -r
racadm sslcertdownload -t 0x1 -f <certificado de
CMC SSL>
```



NOTA: Solo se puede utilizar este comando mediante RACADM remoto. Para obtener más información sobre RACADM remoto, ver “Acceso a RACADM de manera remota” en la página 85.

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 del host del certificado firmado por una autoridad de certificados no se compara con el nombre del servidor especificado. Esto resulta especialmente útil para los administradores del CMC porque permite ingresar un nombre de host además de una dirección IP.


Después de activar la opción **Especificar servidor**, puede especificar un servidor LDAP y un catálogo global con direcciones IP o nombres completos de dominios (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 podrá buscar un servidor.

 **NOTA:** Puede 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, pueden producirse 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 por 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 del DNS primario>
```

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

De esta forma quedará configurada la función de esquema extendido.

Preguntas frecuentes

Tabla 8-9. Uso del CMC con Active Directory: Preguntas frecuentes

Pregunta	Respuesta
¿Puedo iniciar sesión en el CMC utilizando Active Directory 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 a través de dominios si se encuentra en modo mixto.
¿El uso del CMC con Active Directory admite varios entornos de dominio?	Sí. El nivel de función del bosque de dominio debe estar en modo Nativo o en modo de Windows 2003. Además, los grupos entre objeto de asociación, objetos de usuario del RAC y objetos del dispositivo del RAC (incluido el objeto de asociación) deben ser grupos universales.

Tabla 8-9. Uso del CMC con Active Directory: Preguntas frecuentes (continuación)

Pregunta	Respuesta
¿Estos objetos extendidos por Dell (objeto de asociación Dell, dispositivo del 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 obliga a crear estos dos objetos en el mismo dominio. Otros objetos pueden estar en dominios diferentes.
¿Hay alguna restricción para la configuración del SSL de la controladora de dominio?	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.
Creé y cargué un certificado de RAC nuevo y ahora la interfaz web no se inicia.	<p>Si utiliza los servicios de certificados de Microsoft para generar el certificado de RAC, existe la posibilidad de que inadvertidamente haya seleccionado la opción Certificado de usuario en lugar de Certificado de web cuando creó el certificado.</p> <p>Para resolver el problema, genere una CSR, cree un certificado web nuevo utilizando los servicios de certificados de Microsoft y cárguelo mediante los siguientes comandos RACADM:</p> <pre>racadm sslcsrngen [-g] [-f {filename}] racadm sslcertupload -t 1 -f {web_sslcert}</pre>

Tabla 8-9. Uso del CMC con Active Directory: Preguntas frecuentes (continuación)

Pregunta	Respuesta
¿Qué debo hacer si no puedo iniciar sesión en el CMC mediante la autenticación de Active Directory? ¿Cómo soluciono el problema?	<p>1 Asegúrese de utilizar el nombre de dominio de usuario correcto y no el nombre de NetBIOS durante el inicio de sesión.</p> <p>2 Si posee una cuenta de usuario del CMC local, inicie sesión en el CMC por medio de sus credenciales locales.</p> <p>Después de que haber iniciado sesión, realice los pasos siguientes:</p> <ul style="list-style-type: none">a Asegúrese de haber seleccionado la casilla de verificación Habilitar Active Directory en la página de configuración de Active Directory del CMC.b En la página de configuración de red del CMC, asegúrese que la configuración de DNS sea correcta.c Asegúrese de haber cargado en el CMC el certificado de Active Directory desde el certificado con firma de la autoridad de certificados raíz de Active Directory.d Verifique los certificados de SSL de la controladora de dominio para asegurarse de que no hayan expirado.e Asegúrese de que lo datos de las opciones Nombre del CMC, Nombre del dominio raíz y Nombre de dominio del CMC coincidan con la configuración del entorno de Active Directory.f Verifique que la contraseña del CMC tenga 127 caracteres como máximo. Si bien el CMC admite contraseñas de hasta 256 caracteres, Active Directory solo admite contraseñas de 127 caracteres como máximo.

Configuración de inicio de sesión único

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 y Windows Server 2008 pueden utilizar Kerberos, un protocolo de autenticación de red, como método de autenticación que permite que los usuarios que han iniciado sesión en el dominio inicien sesión automáticamente o con un inicio de sesión único en las aplicaciones posteriores, por ejemplo, en Exchange.

A partir de la versión 2.10 del CMC, este puede utilizar Kerberos para admitir dos tipos más de mecanismos de inicio de sesión: el inicio de sesión único y el inicio de sesión mediante tarjeta inteligente. Para el inicio de sesión único, el CMC utiliza las credenciales del sistema cliente, que el sistema operativo almacena en la caché después de haber iniciado sesión desde una cuenta de Active Directory válida.



NOTA: Cuando se selecciona un método de inicio de sesión no se fijan atributos de política respecto de otras interfaces de inicio de sesión, por ejemplo, SSH. También se deben establecer los atributos de política para las otras interfaces de inicio de sesión. Para desactivar todas las otras interfaces de inicio de sesión, vaya a la página [Servicios](#) y desactive todas las interfaces de inicio de sesión (o algunas de ellas).

Requisitos del sistema

Para utilizar la autenticación de Kerberos, la red debe incluir:

- Servidor DNS
- Servidor de Microsoft Active Directory



NOTA: Si utiliza Active Directory en Windows 2003, verifique que tiene el service pack y las actualizaciones más recientes instalados en el sistema cliente. Si está utilizando Active Directory en Windows 2008, verifique que tiene instalado el SP1 junto con las siguientes correcciones urgentes: **Windows6.0-KB951191-x86.msu** para la utilidad KTPASS. Sin esta actualización, la utilidad genera archivos keytab *con errores*. **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

- Para el inicio de sesión mediante tarjeta inteligente únicamente, el cliente debe contar con Microsoft Visual C++ 2005 redistribuible. Para obtener más información, ver www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en
- Para inicio de sesión único e 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 firmware versión 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.

Configuración de valores

Prerrequisitos

- El territorio de Kerberos y su centro de distribución de claves (KDC) para Active Directory han sido configurados (ksetup).
- Una sólida infraestructura de NTP y DNS para evitar problemas de desfase de tiempo y búsqueda inversa.
- El grupo de funciones del esquema estándar del CMC con miembros autorizados.

Configuración de Active Directory

En el cuadro de diálogo **Propiedades del CMC** en la sección de opciones de **Cuentas**, configure estos valores:

- **Se confía en la cuenta para su delegación:** actualmente el CMC no utiliza credenciales reenviadas que se crean cuando se selecciona esta opción. Se puede seleccionar esta opción o no, en función de los requerimientos de otros servicios.
- **La cuenta es importante y no se puede delegar:** esta opción se puede seleccionar o no, en función de los requerimientos de otros servicios.
- **Usar tipos de cifrado DES de Kerberos para esta cuenta:** seleccione esta opción.
- **No pedir la autenticación Kerberos previa:** no seleccione esta opción.

Ejecute la utilidad `ktpass` (parte de Microsoft Windows) en la controladora de dominio (servidor de Active Directory) donde desee asignar el CMC a una cuenta de usuario en Active Directory. Por ejemplo:

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



NOTA: El `nombredemc.nombre_dominio.com` debe estar en minúsculas como exige RFC y el nombre del TERRITORIO, `@REALM_NAME` debe estar en mayúsculas. Además, el CMC admite el tipo de cifrado DES-CBC-MD5 para la autenticación de Kerberos.

Este procedimiento produce un archivo `keytab` que se debe cargar en el CMC.



NOTA: Este archivo contiene una clave de cifrado y debe guardarse de manera segura. Para obtener más información sobre la utilidad `ktpass`, visite el sitio web de Microsoft en: technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.msp?mfr=true

Configuración del CMC



NOTA: Los pasos de configuración que se describen en esta sección solo se aplican al acceso web del CMC.

Configure el CMC para utilizar el grupo o los grupos de funciones del esquema estándar establecidos en Active Directory. Para obtener más información, consulte “Configuración de Active Directory con esquema estándar para acceder al CMC” en la página 284.

Cómo cargar el archivo keytab de Kerberos

El archivo keytab de Kerberos sirve como credenciales del nombre de usuario y la contraseña del CMC para el centro de datos de Kerberos (KDC), que a su vez autoriza el acceso al Active Directory. Cada CMC dentro del territorio de Kerberos se debe registrar con Active Directory y debe tener un archivo keytab exclusivo.

Para cargar el archivo keytab:

- 1 Acceda a la ficha **Autenticación de usuarios**→ subficha **Servicios de directorios**. Asegúrese de que esté seleccionado **Microsoft Active Directory esquema estándar** o bien **esquema extendido**. Si no es así, seleccione la opción que prefiera y haga clic en **Aplicar**.
- 2 Haga clic en **Examinar** en la sección **Carga del archivo keytab de Kerberos**, acceda a la carpeta donde se guarda el archivo keytab y haga clic en **Cargar**.

Al completarse la carga, aparece un cuadro de mensaje que indica que la carga ha sido correcta o ha fallado.

Activación del inicio de sesión único

- 1 Haga clic en la ficha **Seguridad de red de Chassis Management Controller**→ **Active Directory**→ **Configurar Active Directory**. Aparecerá la página **Configuración y administración de Active Directory**.

2 En la página **Configuración y administración de Active Directory**, seleccione:

- Inicio de sesión único: esta opción permite iniciar sesión en el CMC con las credenciales almacenadas en caché que se obtienen al iniciar sesión en Active Directory.



NOTA: Todas las interfaces fuera de banda de línea de comando, incluidas Secure Shell (SSH), Telnet, serie y RACADM remoto se mantienen sin cambio para esta opción.

3 Desplácese al final de la página y haga clic en **Aplicar**.

Es posible probar el Active Directory con autenticación Kerberos mediante la función de prueba de comandos de CLI.

```
testfeature -f adkrb -u <usuario>@<dominio>
```

donde usuario es una cuenta de usuario de Active Directory válida.

Una ejecución satisfactoria del comando indica que el CMC puede adquirir las credenciales Kerberos y acceder a la cuenta del usuario en Active Directory. Si el comando no se ejecuta satisfactoriamente, resuelva el error y repita el comando. Para obtener más información consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC6 y CMC) en support.dell.com/manuals.

Configuración del explorador para inicio de sesión único

El inicio de sesión único 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 autenticación 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 **Opciones avanzadas**.


Se muestra el cuadro de diálogo **Configuración avanzada de Intranet local**.

- 5 En el campo **Agregar este sitio a la zona**, escriba el nombre del CMC y el dominio al cual pertenece y haga clic en **Agregar**.

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

Mozilla Firefox

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

 **NOTA:** Si el explorador muestra el aviso **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**.

Conexión al CMC mediante inicio de sesión único

 **NOTA:** No se puede utilizar la dirección IP para acceder al inicio de sesión único o al inicio de sesión mediante tarjeta inteligente. Kerberos valida las credenciales contra el nombre del dominio completamente expresado (FQDN).

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

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

- 2 Acceda a la página web del CMC utilizando

https://<cmcname.nombre-dominio>

Por ejemplo: **cmc-6G2WXF1.cmcad.1ab**

donde **cmc-6G2WXF1** es el nombre del CMC

cmcad.1ab es el nombre del dominio.



NOTA: Si ha cambiado el número del puerto HTTPS predeterminado (puerto 80), acceda a la página web del CMC utilizando `<cmcname.nombre-dominio>:<número de puerto>`, donde el **cmcname** es el nombre de host del CMC, **nombre-dominio** es el nombre del dominio y **número de puerto** es el número del puerto HTTPS.

Se muestra la página de Inicio de sesión único del CMC.

3 Haga clic en Inicio de sesión.

El CMC lo conecta 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 solo una página en blanco.

Configuración de la autenticación de dos factores de tarjeta inteligente

Los esquemas tradicionales de autenticación utilizan nombres de usuario y contraseña para autenticar a los usuarios. Por el contrario, la autenticación de dos factores proporciona un nivel de seguridad más alto gracias a que requiere que los usuarios tengan una contraseña o PIN y una tarjeta física con una clave privada o un certificado digital. Kerberos, un protocolo de autenticación de red, utiliza este mecanismo de autenticación de dos factores que permite que los sistemas demuestren su autenticidad. Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista y Windows Server 2008 utilizan Kerberos como método de autenticación preferido. A partir de la versión 2.10 del CMC, este puede utilizar Kerberos para permitir el inicio de sesión mediante tarjeta inteligente.



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

Requisitos del sistema


Los “Requisitos del sistema” en la página 314 para la tarjeta inteligente son los mismos que para el inicio de sesión único.

Configuración de valores


Los “Prerrequisitos” en la página 315 para la tarjeta inteligente son los mismos que para el inicio de sesión único.

Configuración de Active Directory

Para configurar Active Directory:

- 1 Configure el territorio de Kerberos y su centro de distribución de claves (KDC) para Active Directory, si aún no han sido configurados (ksetup).
 **NOTA:** Procure tener una sólida infraestructura de NTP y DNS para evitar problemas de desfase de tiempo y búsqueda inversa.
- 2 Cree usuarios de Active Directory para cada CMC, configurados para utilizar el cifrado DES de Kerberos pero no la preautenticación.
- 3 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).

Configuración del CMC

 **NOTA:** Los pasos de configuración que se describen en esta sección solo se aplican al acceso web del CMC.

Configure el CMC para utilizar el grupo o los grupos de funciones del esquema estándar establecidos en Active Directory. Para obtener más información, consulte “Configuración de Active Directory con esquema estándar para acceder al CMC” en la página 284.

Cómo cargar el archivo keytab de Kerberos


El archivo keytab de Kerberos sirve como credenciales del nombre de usuario y la contraseña del CMC para el centro de datos de Kerberos (KDC), que a su vez autoriza el acceso al Active Directory. Cada CMC dentro del territorio de Kerberos se debe registrar con Active Directory y debe tener un archivo keytab exclusivo.

Para cargar el archivo keytab:

- 1 Acceda a la ficha **Autenticación de usuarios**→ subficha **Servicios de directorios**. Asegúrese de que esté seleccionado **Microsoft Active Directory esquema estándar** o bien **esquema extendido**. Si no es así, seleccione la opción que prefiera y haga clic en **Aplicar**.
- 2 Haga clic en **Examinar** en la sección **Carga de archivo keytab de Kerberos**, acceda a la carpeta donde se guarda el archivo keytab y haga clic en **Cargar**. Al completarse la carga, aparece un cuadro de mensaje que indica que la carga ha sido correcta o ha fallado.

Activación de la autenticación de tarjeta inteligente

Para activar la autenticación de tarjeta inteligente:

- 1 Acceda a la ficha **Autenticación de usuarios**→ subficha **Servicios de directorios**. Asegúrese de que esté seleccionado **Microsoft Active Directory esquema estándar** o bien **esquema extendido**.
 - 2 En la sección **Valores comunes**, seleccione:
 - Tarjeta inteligente: esta opción requiere insertar una tarjeta inteligente en el lector e introducir el número de PIN.
-  **NOTA:** Todas las interfaces fuera de banda de línea de comando, incluidas Secure Shell (SSH), Telnet, serie y RACADM remoto se mantienen sin cambio para esta opción.
- 3 Desplácese al final de la página y haga clic en **Aplicar**.

Es posible comprobar Active Directory con autenticación Kerberos mediante la función de prueba de comandos de CLI.

Escriba:

```
testfeature -f adkrb -u <usuario>@<dominio>
```

donde *usuario* es una cuenta de usuario de Active Directory válida.

Una ejecución satisfactoria del comando indica que el CMC puede adquirir las credenciales Kerberos y acceder a la cuenta del usuario en Active Directory. Si el comando no se ejecuta satisfactoriamente, resuelva el error y repita el comando. Para obtener más información, consulte la documentación relacionada con el comando testfeature de RACADM.

Configuración del explorador para el inicio de sesión mediante tarjeta inteligente

Mozilla Firefox

El CMC 2.10 no admite el inicio de sesión mediante tarjeta inteligente mediante el explorador Firefox.

Internet Explorer

Verifique que Internet Explorer esté configurado para descargar los complementos Active-X.

Cómo iniciar sesión en el CMC mediante una tarjeta inteligente



NOTA: No se puede utilizar la dirección IP para acceder al inicio de sesión único o al inicio de sesión mediante tarjeta inteligente. Kerberos valida las credenciales contra el nombre del dominio completamente expresado (FQDN).

Para iniciar sesión en el CMC mediante una tarjeta inteligente:

- 1 Inicie sesión en el sistema cliente utilizando su cuenta de red.
- 2 Acceda a la página web del CMC utilizando `https://<cmcname.nombre-dominio>`

Por ejemplo: `cmc-6G2WXF1.cmcad.lab`

donde `cmc-6G2WXF1` es el nombre del CMC

`cmcad.lab` es el nombre del dominio.



NOTA: Si ha cambiado el número del puerto HTTPS predeterminado (puerto 80), acceda a la página web del CMC utilizando `<cmcname.nombre-dominio>:<número de puerto>`, donde el nombre de `cmc` es el nombre de host del CMC, `nombre-dominio` es el nombre del dominio y `número de puerto` es el número del puerto HTTPS.

Se muestra la página **Inicio de sesión único del CMC** que le indica que debe insertar la tarjeta inteligente.

- 3 Inserte la tarjeta inteligente en el lector y haga clic en **Aceptar**.
Se abrirá el cuadro de diálogo **emergente** para introducir el PIN.

- 4 De forma opcional, puede seleccionar un límite de tiempo de espera para la sesión. Este es el plazo en el que puede permanecer conectado sin actividad. El valor predeterminado se define como el tiempo de espera en inactividad del servicio web. Para obtener más información, consulte Configuración de servicios.
- 5 Introduzca el PIN y haga clic en **Aceptar**.

Solución de problemas del inicio de sesión mediante tarjeta inteligente

Utilice los siguientes consejos y sugerencias como ayuda para depurar una tarjeta inteligente que no permite el acceso:

El complemento ActiveX no puede detectar el lector de tarjetas Smart

Verifique que la tarjeta inteligente sea compatible con el sistema operativo Microsoft Windows. Windows admite una cantidad limitada de proveedores de servicios de cifrado (CSP) de tarjetas inteligente.

Como verificación general para determinar si los CSP de tarjetas inteligentes están presentes en un cliente específico, inserte la tarjeta inteligente en el lector con la pantalla de inicio de sesión (Ctrl-Alt-Supr) de Windows y compruebe si Windows detecta la tarjeta inteligente y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente

Revise si la tarjeta inteligente se bloqueó debido a que se hicieron demasiados intentos con PIN incorrectos. En tales casos, el emisor de la tarjeta inteligente en la organización podrá ayudarle a obtener una nueva tarjeta inteligente.

No se puede iniciar sesión en el CMC como usuario de Active Directory

Si no puede iniciar sesión en el CMC como usuario de Active Directory, trate de iniciar sesión en el CMC sin activar el inicio de sesión mediante tarjeta inteligente. También tiene la opción de desactivar el inicio de sesión mediante tarjeta inteligente a través de RACADM local con los siguientes comandos:

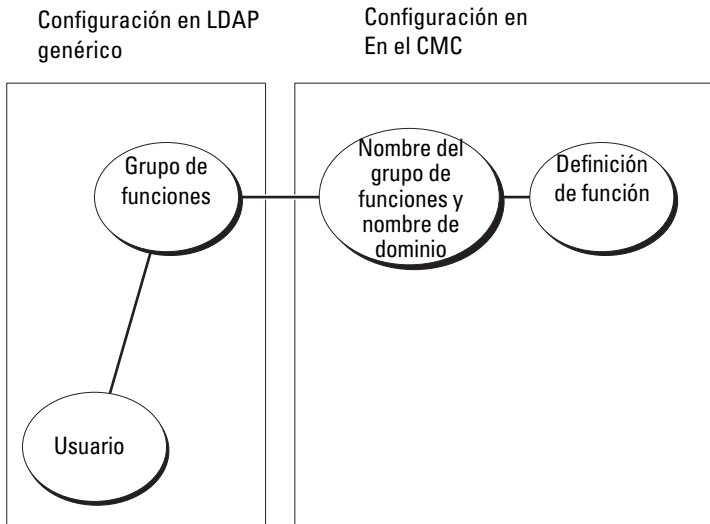
```
racadm config -g cfgActiveDirectory -o cfgADSCLEnable 0  
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0
```

Uso del CMC con LDAP genérico

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

Para permitir que el usuario de LDAP acceda a una tarjeta de CMC específica, el nombre del grupo de funciones y su nombre de dominio deben estar configurados en la tarjeta. Puede configurar un máximo de cinco grupos de funciones en cada CMC. La Tabla 5-43 muestra el nivel de privilegios de los grupos de funciones y la Tabla 8-1 muestra la configuración predeterminada del grupo de funciones. Ilustración 8-5 muestra la configuración de CMC con LDAP genérico

Ilustración 8-5. Configuración de CMC con LDAP genérico



Configuración del directorio LDAP genérico para acceder a CMC

La implementación del LDAP genérico del CMC utiliza dos etapas para otorgar acceso a un usuario. La etapa 1 comienza con la autenticación del usuario y luego sigue la etapa 2 de autorización del usuario.

Autenticación y autorización de usuarios de LDAP

Algunos servidores de directorios requieren un enlace para poder realizar búsquedas en un servidor LDAP específico. Los pasos de la autenticación son:

- 1 De forma opcional, establecer un enlace con el servicio de directorio. La opción predeterminada es un enlace anónimo.
- 2 Buscar el usuario con base en su inicio de sesión. El atributo predeterminado es **uid**.
- 3 Si se encuentra más de un objeto, el proceso arroja un mensaje de error.
- 4 Desvincular y establecer un enlace con el DN y la contraseña del usuario.
- 5 Si el enlace falla, fallará el inicio de sesión.

Si estos pasos se completan satisfactoriamente, el usuario se considera autenticado. La siguiente etapa es la autorización. El CMC almacena un máximo de 5 grupos con sus correspondientes privilegios. Un usuario tiene la opción de ser agregado a múltiples grupos en el servicio de directorio. Si el usuario es miembro de varios grupos, obtiene los privilegios de todos esos grupos.

Los pasos de la autorización son:

- 1 Buscar en cada grupo configurado el DN del usuario en los atributos de **miembro** o **uniqueMember**. Este campo puede ser configurado por el administrador.
- 2 Para cada grupo al que pertenece el usuario, agregar sus privilegios juntos.

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web del CMC

Puede utilizar el servicio genérico de Protocolo ligero de acceso a directorios (LDAP) para configurar el software para que proporcione acceso al CMC. El servicio LDAP le permite agregar y controlar los privilegios de los usuarios existentes del CMC.



NOTA: Para configurar los valores de LDAP para el CMC, debe tener privilegios de **Administrador de configuración del chasis**.

Para obtener más información sobre la configuración de LDAP genérico, ver “Uso del CMC con LDAP genérico” en la página 325.

Para ver y configurar LDAP:

- 1 Inicie sesión en la interfaz web.
- 2 Haga clic en la ficha **Autenticación de usuarios** y luego en la subficha **Servicios de directorios**. Aparecerá la página **Servicios de directorios**.
- 3 Haga clic en el botón de radio relacionado con LDAP genérico.
- 4 Configure las opciones que aparecen y haga clic en **Aplicar**.

Tabla 8-10 muestra las opciones disponibles:

Tabla 8-10. Valores comunes

Valor	Descripción
LDAP genérico activado	Activa el servicio LDAP genérico en el CMC.
Usar nombre distintivo para buscar la pertenencia a grupos	Especifica el nombre distintivo (DN) de los grupos LDAP cuyos miembros tienen permiso para acceder al dispositivo.
Activar validación de certificados de SSL	Si esta opción está marcada, el CMC utiliza el certificado de CA para validar el certificado del servidor LDAP durante el protocolo de enlace de SSL.
DN de enlace	Especifica el nombre distintivo de un usuario que se utiliza para establecer un enlace con el servidor cuando busca el DN de usuario de inicio de sesión. Si no se indica, se utiliza un enlace anónimo.
Contraseña	Contraseña de enlace para utilizar junto con el DN de enlace. NOTA: La contraseña de enlace es información confidencial, por lo que debe estar protegida correctamente.
DN de base para buscar	Es el nombre de dominio de la rama del directorio donde deben iniciarse todas las búsquedas.
Atributo de inicio de sesión del usuario	Especifica el atributo que hay que buscar. Si no ha sido configurado, la opción predeterminada es utilizar uid. Se recomienda que sea único dentro del DN de base seleccionado, pues de lo contrario será necesario configurar un filtro de búsqueda para garantizar que el usuario sea único. Si el DN del usuario no puede ser identificado en forma exclusiva por la combinación de atributo y filtro de búsqueda, el inicio de sesión fallará.

Tabla 8-10. Valores comunes (continuación)

Valor	Descripción
Atributo de pertenencia a grupos	Especifica el atributo de LDAP que se utiliza para verificar la pertenencia a grupos. Este deberá ser un atributo de la clase de grupos. Si se especifica, se utilizan los atributos de miembro y miembro único.
Filtro de búsqueda	Especifica un filtro de búsqueda de LDAP válido. Se utiliza cuando el atributo del usuario no puede identificar de forma exclusiva al usuario dentro del DN de base seleccionado. Si no se especifica, el valor predeterminado es (objectClass=*), que busca todos los objetos en el árbol. La longitud máxima de esta propiedad es de 1024 caracteres.
Tiempo de espera de la red (segundos)	Define el tiempo (expresado en segundos) que debe transcurrir para que una sesión inactiva de LDAP se cierre automáticamente.
Tiempo de espera de búsqueda (segundos)	Define el tiempo (expresado en segundos) que debe transcurrir para que una búsqueda se cierre automáticamente.

Selección de servidores LDAP

Puede configurar el servidor que utilizará con LDAP genérico de dos maneras. Los servidores estáticos le permiten al administrador colocar un nombre de dominio completamente expresado (FQDN) o una dirección IP en el campo. De forma alternativa, puede obtenerse una lista de servidores LDAP si se buscan sus registros de SRV en los DNS.

En la sección de servidores LDAP se muestran las siguientes propiedades:

- Usar servidores LDAP estáticos: al seleccionar esta opción, el servicio LDAP utiliza los servidores especificados con el número de puerto proporcionado (consulte la información a continuación).



NOTA: Debe seleccionar la opción de servidor estático o DNS.

- Dirección del servidor LDAP: permite especificar el FQDN o la dirección IP del servidor LDAP. Para especificar múltiples servidores LDAP redundantes que tienen a disposición el mismo dominio, proporcione la lista de todos los servidores separados por comas. CMC intenta conectar a cada servidor, uno por uno, hasta que logra una conexión exitosa.

- Puerto del servidor LDAP: es el puerto de LDAP a través de SSL, que de forma predeterminada será el 636 si no se configura la opción. En CMC versión 3.0 no se admite el uso de puertos que no sean SSL, ya que la contraseña no puede transportarse sin SSL.
- Usar DNS para encontrar servidores LDAP: Al seleccionar esta opción, LDAP utiliza el dominio de búsqueda y el nombre de servicio a través de DNS. Debe seleccionar la opción de servidor estático o DNS.

Se ejecutará la siguiente consulta de DNS para los registros de SRV:

_<Nombre de servicio>._tcp.<Dominio de búsqueda>

donde *<Dominio de búsqueda>* es el dominio de nivel raíz que se utiliza en la consulta y *<Nombre de servicio>* indica el nombre del servicio a 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.

Administración de la configuración de grupo de LDAP

La tabla de la sección Configuración de grupo muestra una lista de los grupos de funciones con nombres, dominios y privilegios relacionados para todo grupo de funciones que ya esté configurado.

- Para configurar un nuevo grupo de funciones, haga clic en el nombre de un grupo que no tenga nombres, dominios ni privilegios.
- Para cambiar la configuración de un grupo de funciones ya existente, haga clic en el nombre del grupo de funciones.

Al hacer clic aparecerá la página **Configurar grupo de funciones**. La ayuda para esa página está disponible mediante el vínculo **Ayuda** en la esquina superior derecha de la página.

Administración de certificados de seguridad de LDAP

Esta sección muestra las propiedades del certificado de LDAP recientemente cargado en el CMC. Si carga un certificado, utilice esta información para verificar que el certificado es válido y no está vencido.



NOTA: De manera predeterminada, el CMC no tiene un certificado de servidor emitido por una autoridad de certificados para Active Directory. Debe cargar un certificado de servidor vigente y firmado por una autoridad de certificados.

Se muestran las siguientes propiedades del certificado:

- Número de serie: el número de serie del certificado.
- Información del titular: el titular del certificado (nombre de la persona o empresa certificada).
- Información del emisor: el emisor del certificado (nombre de la autoridad de certificados).
- Válido desde: indica la fecha de inicio del certificado.
- Válido hasta: indica la fecha de vencimiento del certificado.

Los siguientes controles le permiten cargar y descargar este certificado:

- Cargar: inicia el proceso de carga del certificado. Este certificado, que se obtiene del servidor LDAP, proporciona acceso al CMC.
- Descargar: inicia el proceso de descarga. El sistema le solicitará que indique una ubicación para guardar el archivo. Cuando seleccione esta opción, haga clic en **Siguiente** y aparecerá el cuadro de diálogo **Descarga de archivo**. Utilice este cuadro de diálogo para especificar una ubicación en la estación de administración o en la red compartida para el certificado de servidor.

Configuración del servicio de directorio LDAP genérico mediante RACADM



NOTA: Esta función admite IPv4 e IPv6.

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 obligatorios incluyen la activación de inicios de sesión de LDAP, la definición del FQDN o la IP del 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 SRV. Si la propiedad `cfgLDAPSRVLookupEnable` está activada, la propiedad `cfgLDAPServer` no se toma en cuenta. La siguiente consulta se utiliza para buscar registros SRV en el DNS:

```
_ldap._tcp.domainname.com
```

En esta consulta, `ldap` es la propiedad `cfgLDAPSRVLookupServiceName`. `cfgLDAPSRVLookupDomainName` se configura para ser `domainname.com`.

Uso

Para iniciar sesión en el CMC mediante un usuario de LDAP, utilice el nombre del usuario en el inicio de sesión y la contraseña del usuario cuando el sistema la solicite. Si un usuario de LDAP no puede iniciar sesión por algún motivo, el CMC retrocede e intenta utilizar un inicio de sesión local con el mismo nombre de usuario y contraseña. Esto permite iniciar sesión aunque no haya conectividad de red o si el servidor LDAP está fuera de alcance.

Obtención de ayuda

El registro de rastreo del CMC contiene cierta información sobre los motivos por los que el usuario no puede iniciar sesión. Para clasificar los intentos fallidos de inicio de sesión, se recomienda utilizar el comando `racadm testfeature -f LDAP` con la función de depuración activada.

Administración de la alimentación

El gabinete del servidor Dell PowerEdge M1000e es el gabinete de servidor modular de menor consumo energético del mercado. Está diseñado para incluir suministros de energía y ventiladores de gran eficiencia, su diseño ha sido optimizado para que el aire circule más fácilmente a través del sistema y todo el gabinete contiene componentes que optimizan el uso de la alimentación. El diseño de hardware optimizado está equipado con sofisticadas capacidades de administración de la alimentación integradas en el Chassis Management Controller (CMC), suministros de energía e iDRAC a fin de permitir mayores mejoras de la eficiencia energética y tener total control sobre el entorno de alimentación eléctrica.

El gabinete modular del PowerEdge M1000e toma corriente alterna y distribuye la carga entre todas las unidades de suministro de energía (PSU) internas y activas. El sistema puede generar hasta 16685 vatios de corriente alterna que se asignan a módulos de servidor y a la infraestructura de gabinete asociada.

La administración de la alimentación también se puede controlar con la **Consola de medición, mitigación y administración de la alimentación (PM3)**. Cuando la PM3 controla la alimentación de forma externa, el CMC mantiene lo siguiente:

- Política de redundancia
- Registro remoto de la alimentación
- Rendimiento del sistema sobre redundancia de alimentación
- Conexión dinámica del suministro de energía
- Operación a 110 V CA

La PM3 administra lo siguiente:

- Alimentación del servidor
- Prioridad de los servidores
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

Para obtener más información, consulte “Administración de la alimentación externa” en la página 382.



NOTA: La entrega real de la alimentación real se basa en la configuración y en la carga de trabajo.

Las funciones de administración de la alimentación del M1000e ayudan a los administradores a configurar el gabinete a fin de reducir el consumo de alimentación y adecuar la administración de la alimentación a sus necesidades y entornos específicos.

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.

Modo de redundancia de CA

El objetivo de la política de redundancia de CA es permitir que un sistema de gabinete modular pueda funcionar de un modo que le permita tolerar las fallas de alimentación de CA. Es posible que estas fallas se originen en la red de corriente alterna, el cableado y el suministro, o en la propia unidad de suministro de energía.

Cuando se configura un sistema para tener redundancia de CA, las unidades de suministro de energía se dividen entre las redes eléctrica: 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 CA también tolera las fallas de las unidades de suministro de energía individuales.



NOTA: Dado que una de las funciones de la redundancia de CA es proporcionar una operación perfecta del servidor a pesar de cualquier falla que se produzca en toda una red eléctrica, la mayor parte de la alimentación se pone a disposición del mantenimiento de la redundancia de CA cuando las capacidades de las dos redes eléctricas son aproximadamente iguales.



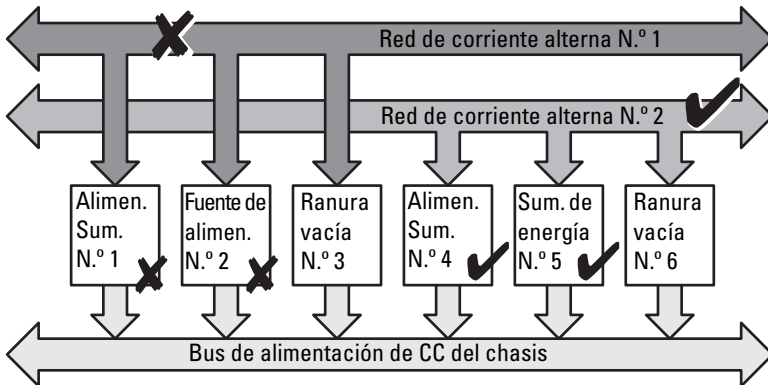
NOTA: La redundancia de CA solo se cumple cuando los requisitos de carga no superan la capacidad de la red eléctrica más débil.

Niveles de redundancia de CA

La configuración mínima necesaria para tener redundancia de CA es tener una unidad de suministro de energía en cada red eléctrica. Es posible definir configuraciones adicionales con cualquier 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 se lo más similar posible. El límite máximo de energía mientras se mantiene la redundancia de CA es la energía disponible en la más débil de las dos redes eléctricas. Ilustración 9-1 muestra dos unidades de suministro de energía por cada red eléctrica y una falla de alimentación en la red eléctrica 1.

Si por alguna razón el CMC no puede mantener la redundancia de CA, se envían alertas de correo electrónico y/o SNMP a los administradores, siempre que el suceso Redundancia perdida esté configurado para el envío de alertas.

Ilustración 9-1. muestra dos unidades de suministro de energía por cada red eléctrica y una falla de alimentación en la red eléctrica 1



NOTA: 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 CA aparecerá como Sin redundancia y la condición del chasis aparecerá como Crítica.

Modo de redundancia de suministro de energía

El modo de redundancia de suministro de energía es útil cuando las redes eléctricas redundantes no están disponibles, pero es recomendable protegerse contra la falla de una sola unidad de suministro de energía que desactive los servidores de un gabinete modular. La unidad de suministro de energía con mayor capacidad se mantiene en reserva en línea para este fin. Esto constituye un grupo de redundancia de suministro de energía. Ilustración 9-2 muestra 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 agregarán 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.


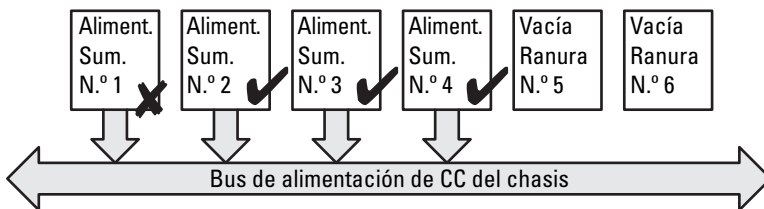
 **NOTA:** La conexión dinámica del suministro de energía (DPSE) permite poner en espera las unidades de suministro de energía. El estado En espera indica una condición física en la que no se suministra alimentación. Al activar DPSE, las unidades de suministro de energía adicionales pueden ponerse en modo de espera para aumentar la eficiencia y ahorrar energía.

Ilustración 9-2. Redundancia de suministro de energía: total de 4 unidades de suministro de energía con la falla de una unidad.



Red eléctrica doble o simple:
La redundancia de suministro de energía protege contra fallas de un suministro de energía único.

Modo sin redundancia

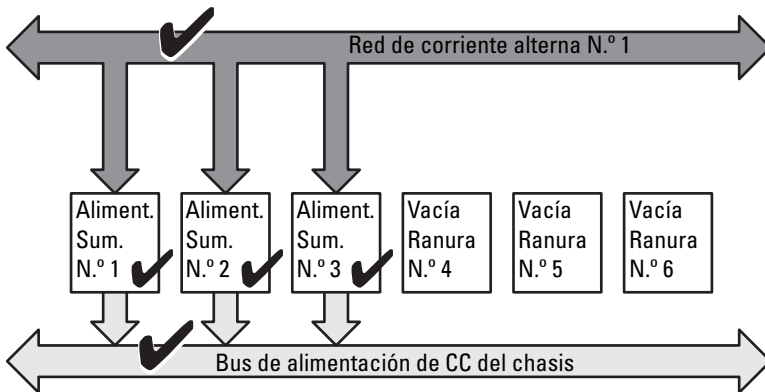
El **modo sin redundancia** es el valor predeterminado de fábrica para la configuración de 3 unidades de suministro de energía e indica que el chasis no tiene redundancia de alimentación configurada. En esta configuración, el estado de redundancia general del chasis indicará siempre **Sin redundancia**. Ilustración 9-3 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 en el modo **Sin redundancia**.



NOTA: Todas las unidades de suministro de energía del chasis aparecerán **En línea** si DPSE está activada durante el modo **Sin redundancia**. Cuando se activa 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 9-3. Sin redundancia con tres unidades de suministro de energía en el chasis



Red eléctrica simple:

No proporciona protección contra fallas de las redes eléctricas o de los suministros de energía.

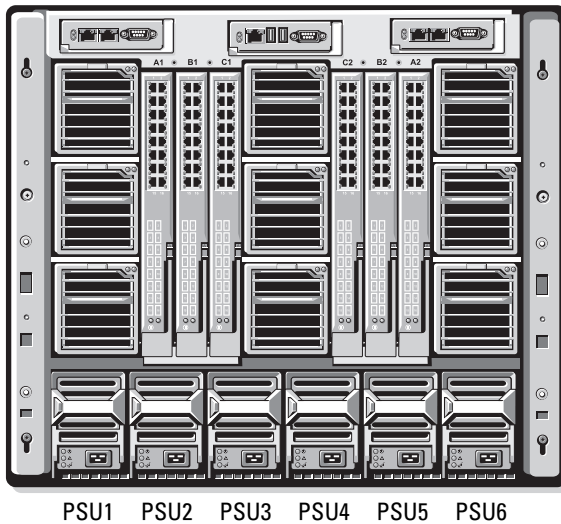
Una falla en una unidad de suministro de energía hace que las demás unidades de suministro de energía salgan del modo En espera, según sea necesario, para cubrir las asignaciones de energía del chasis. Si existen cuatro unidades de suministro de energía y solo se requieren tres, en caso de que una falle una, 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 “Conexión dinámica del suministro de energía” en la página 342.

Presupuesto de alimentación para módulos de hardware

La Ilustración 9-4 muestra un chasis con una configuración de seis unidades de suministro de energía. Las unidades de suministro de energía se numeran de 1 a 6 a partir del lado izquierdo del gabinete.

Ilustración 9-4. 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 están presentes). El chasis puede contener hasta 16 servidores que se comunican con el chasis mediante iDRAC. Para obtener más información, consulte la *Guía del usuario de iDRAC* en support.dell.com/manuals.

El iDRAC proporciona al CMC el requisito de máxima potencia antes de encender el servidor. La envoltura 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 descubrir otros componentes, el iDRAC puede aumentar o reducir sus requisitos de alimentación iniciales.

Cuando se enciende un servidor en un gabinete, el software del iDRAC vuelve a calcular los requisitos de alimentación y solicita el cambio correspondiente en la envoltura 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 envoltura 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 consumirán 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 lo hay) 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 del **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 con base en 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
- Server (Servidor)
- Módulo de E/S
- Retiro de 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.



NOTA: Al insertar un servidor con otra geometría que no sea una altura simple y si no hay suficiente alimentación para el iDRAC, el servidor aparece como varios servidores de altura simple.

Valores de prioridad de alimentación de ranura del servidor

El CMC permite que los usuarios definan una prioridad de alimentación para cada una de las dieciséis 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 al 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 obtendrán 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, lo que depende del valor mínimo en el que se establece 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 están presentes) 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.

Conexión dinámica del suministro 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 evita que se genere demasiado calor.

El CMC supervisa la asignación total de alimentación del gabinete y coloca las unidades de suministro de energía en el estado **En espera**, lo que provoca que la asignación de alimentación total del chasis se realice a través de menos unidades de suministro de energía. Debido a que las unidades de suministro de energía son más eficientes cuando funcionan mayor capacidad, esto mejora su eficiencia al mismo tiempo que mejora la longevidad de las unidades de suministro de energía 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, con una unidad de suministro de energía requerida para alimentar la configuración y otra para proporcionar redundancia en caso de falla de la unidad de suministro de energía. El modo **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 CA** 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 todas las seis fuentes están activas y comparten la carga, lo cual produce una utilización más baja de cada suministro de energía.

La DPSE puede activarse para las tres configuraciones de redundancia de suministro de energía explicadas anteriormente: **Sin redundancia**, **Redundancia de suministro de energía** y **Redundancia de CA**.

- 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 ocasionará que un modo **En espera** se convierta en **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 y aún tener suficiente energía para los módulos de servidor instalados. La pérdida de la unidad de suministro de energía en línea hará que una unidad en espera 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 **Redundancia de CA**, todos los suministros de energía están activos al encenderse el chasis. El uso de la energía se supervisa y, si la configuración del sistema y el consumo de alimentación lo permiten, las unidades de suministro de energía se ponen en el estado **En espera**. Debido a que el modo **En línea** en una red eléctrica refleja el modo de la otra red eléctrica, el gabinete puede sobrellevar la pérdida de alimentación de una red eléctrica completa sin interrumpir de alimentación en el gabinete.

Un aumento de la demanda de energía en la configuración de **Redundancia de CA** 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.

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 CA
- Redundancia de suministro de energía
- Sin redundancia

La configuración de redundancia predeterminada para un chasis depende de la cantidad de unidades de suministro de energía que contenga, como se muestra en la Tabla 9-1.

Tabla 9-1. 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 CA	Desactivado
Tres unidades de suministro de energía	Sin redundancia	Desactivado

Redundancia de CA

En el modo de redundancia de CA 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 CA, mientras que las tres unidades de suministro de energía de la derecha deben estar conectadas a otra red de CA.

△ PRECAUCIÓN: Para evitar una falla del sistema y para que la redundancia de CA funcione de manera eficaz, debe haber un conjunto equilibrado de unidades de suministro de energía correctamente cableadas a redes de CA independientes.

Si una red de CA falla, las unidades de suministro de energía de la red de CA en funcionamiento tomarán el control sin interrupción para los servidores o la infraestructura.

△ PRECAUCIÓN: En el modo de redundancia de CA, 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 CA no será posible.

Redundancia de 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 está 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, si falla una única unidad de suministro de energía los servidores podrían perder energía y datos.

Conservación de la energía y cambios en el presupuesto de alimentación

El CMC puede llevar a cabo la conservación de 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 para liberar energía y enviarla a los servidores de mayor prioridad y otros módulos del chasis.

Si todas o varias ranuras del chasis están configuradas con el mismo nivel de prioridad, 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 de servidor del 1 al 9 inclusive. El nivel de prioridad predeterminado para todos los servidores es 1. Cuanto menor es el número, mayor es el nivel de prioridad.

Para obtener instrucciones acerca de cómo asignar niveles de prioridad a los servidores, ver “Cómo utilizar de RACADM” en la página 373.

Puede asignar el nivel de prioridad de los servidores utilizando la interfaz gráfica de usuario:

- 1 Haga clic en **Servidores** en el árbol del sistema.
- 2 Haga clic en **Alimentación**→ **Prioridad**.

Conservación de la energía y modo de conservación máxima

El CMC realiza una conservación máxima de la energía en los siguientes casos:

- El usuario selecciona el modo de conservación máxima por medio de la interfaz web o RACADM.
- Una secuencia de línea de comandos automatizada emitida por una fuente de alimentación ininterrumpible selecciona 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 rendimiento completo del sistema se restablece cuando el usuario o una secuencia de línea de comandos automatizada deseleccionan el modo de conservación máxima.

Cómo utilizar la interfaz web

Puede seleccionar o deseleccionar el modo de conservación máxima de la energía por medio de la interfaz gráfica de usuario:

- 1 Haga clic en **Descripción general del chasis** en el árbol del sistema.
- 2 Haga clic en **Alimentación** → **Configuración**.
- 3 Seleccione la casilla **Modo de conservación máxima de la energía** para activar este modo y haga clic en **Aplicar**.
- 4 Deje sin seleccionar la casilla **Modo de conservación máxima de la energía** para restablecer el funcionamiento normal y haga clic en **Aplicar**.

Cómo utilizar de RACADM

Abra una consola serie/Telnet/SSH en CMC e inicie sesión.

- 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
```

Operación de unidades de suministro de energía de 110 V

Algunas unidades de suministro de energía admiten operación con una entrada de 110 V 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 CA, el usuario deberá configurar el CMC para el funcionamiento normal del gabinete. 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 RACADM.

Cómo utilizar la interfaz web

Verifique que el circuito de 110 V tenga capacidad para la corriente estimada y realice los siguientes pasos:

- 1 Haga clic en **Descripción general del chasis** en el árbol del sistema.
- 2 Haga clic en **Alimentación** → **Configuración**.
- 3 Seleccione **Permitir operación con 110 V CA** y haga clic en **Aplicar**.

Cómo utilizar de RACADM

Verifique que el circuito de 110 V tenga capacidad para la corriente calculada y realice los siguientes pasos:

- 1 Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
- 2 Active las unidades de suministro de energía de 110 V CA:

```
racadm config -g cfgChassisPower -o  
cfgChassisAllow110VACOperation 1
```

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 suministros de energía del chasis no proporcionan suficiente alimentación tanto para redundancia como para el rendimiento total, si se quiere preservar redundancia, es posible que algunos servidores no dispongan de lo siguiente:

- Suficiente alimentación para un rendimiento completo.
- Encendido

Cómo utilizar la interfaz web

Siga los pasos siguientes para activar el rendimiento del servidor sobre redundancia de alimentación:

- 1** Haga clic en **Descripción general del chasis** en el árbol del sistema.
- 2** Haga clic en **Alimentación**→ **Configuración**.
- 3** Seleccione **Rendimiento de servidor por encima de redundancia de alimentación** y haga clic en **Aplicar**.

Siga los pasos siguientes para desactivar el rendimiento del servidor sobre redundancia de alimentación:

- 1** Haga clic en **Descripción general del chasis** en el árbol del sistema.
- 2** Haga clic en **Alimentación**→ **Configuración**.
- 3** Deseleccione **Rendimiento de servidor por encima de redundancia de alimentación** y haga clic en **Aplicar**.

Cómo utilizar de RACADM

Siga los pasos siguientes para activar el rendimiento del servidor sobre redundancia de alimentación:

- 1** Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
- 2** Rendimiento del sistema sobre redundancia de alimentación:

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

Siga los pasos siguientes para desactivar el rendimiento del servidor sobre redundancia de alimentación:

- 1** Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
- 2** Desactive Rendimiento del sistema sobre redundancia de alimentación:

```
racadm config -g cfgChassisPower -o  
cfgChassisPerformanceOverRedundancy 0
```

Registro remoto

Se puede informar sobre el consumo de alimentación a un servidor de registro de sistema remoto. En el registro puede aparecer información sobre el consumo total del chasis, el consumo de alimentación mínimo, máximo y medio en un periodo determinado. Para obtener más información sobre la manera de activar esta función y configurar el intervalo de recopilación y registro, consulte las secciones siguientes.

Cómo utilizar la interfaz web

Puede activar el registro de alimentación remoto mediante la interfaz gráfica de usuario. Para ello deberá iniciar sesión en la interfaz y hacer lo siguiente:

- 1 Haga clic en **Descripción general del chasis** en el árbol del sistema.
- 2 Haga clic en **Alimentación** → **Configuración**.
- 3 Seleccione **Registro remoto de alimentación** para poder registrar sucesos de alimentación en un host remoto.
- 4 Especifique el intervalo de registro necesario (de 1 a 1.440 minutos).
- 5 Haga clic en **Aplicar** para guardar los cambios.

Cómo utilizar de RACADM

Abra una consola de texto SSH, de serie o Telnet en CMC, inicie sesión y configure el registro remoto de alimentación como se muestra a continuación:

- 1 Para activar la función de registro remoto de alimentación, introduzca el comando siguiente:

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingEnabled 1
```

- 2 Para especificar el intervalo de registro deseado, introduzca el comando siguiente:

```
racadm config -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingInterval n
```

donde n es un valor de 1 a 1.440 minutos.

- 3 Para comprobar que la función de registro remoto de alimentación está activada, introduzca el comando siguiente:

```
racadm getconfig -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingEnabled
```

- 4 Para determinar el intervalo de registro remoto de alimentación, introduzca el comando siguiente:

```
racadm getconfig -g cfgRemoteHosts -o  
cfgRhostsSyslogPowerLoggingInterval
```



NOTA: La función de registro remoto de alimentación depende de que los hosts de registro de sistema remoto se hayan configurado previamente. Se debe activar el registro a uno o varios host de registro de sistema remoto, de lo contrario se registrará el consumo de alimentación. Esto se puede realizar mediante la interfaz gráfica de usuario o el CLI de RACADM. Para obtener más detalles consulte las instrucciones de configuración del registro de sistema remoto.

Fallo de 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 para los servidores con mayor prioridad se restaura en incrementos mientras las necesidades de alimentación permanecen dentro del presupuesto de alimentación.



NOTA: Para establecer la política de redundancia, ver “Configuración del presupuesto y la redundancia de alimentación” en la página 369.

Política de conexión de servidores nuevos

Cuando se enciende un servidor nuevo, es posible que el CMC tenga que reducir la alimentación a los servidores con menor prioridad para proporcionar más alimentación al servidor nuevo si la adición del nuevo servidor supera la alimentación disponible para el chasis. Esto podría suceder si el administrador ha configurado un límite de alimentación para el chasis que es menor de lo que se requeriría para la asignación de toda la alimentación a los servidores, o si no hay alimentación suficiente para la mayor necesidad de alimentación posible de todos los servidores del 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, entonces no se asignará a ningún servidor alimentación menor a la que se necesita para el peor de los casos y el nuevo servidor se podrá encender.

Si el requisito de alimentación del peor de los casos no se puede cumplir, la alimentación de los servidores con menor prioridad se reducirá hasta liberar suficiente alimentación para iniciar el nuevo servidor.

La Tabla 9-2 describe las acciones realizadas por el CMC cuando se enciende un nuevo servidor en las condiciones descritas anteriormente.

Tabla 9-2. 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 realiza la conservación de energía: <ul style="list-style-type: none"> • La alimentación requerida para el nuevo servidor está disponible • La alimentación requerida para el nuevo servidor no está disponible 	Permitido No permitido

Si una unidad de suministro de energía falla, se produce un estado no crítico y se genera un suceso de falla de unidad de suministro de energía. Al quitar una unidad de suministro de energía se genera un suceso de retiro de unidad de suministro de energía.

Si uno de los sucesos ocasiona una pérdida de redundancia, con base en 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 e incluso podrían llegar a apagarse. Ambas condiciones se dan en orden de prioridad inverso, es decir, los servidores de menor prioridad se apagan primero.

La Tabla 9-3 describe la respuesta del firmware al 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 9-3. Impacto en el chasis de la falla o el desmontaje de una unidad de suministro de energía

Configuración de unidades de suministro de energía	Unidad de suministro de energía dinámica Conexión	Respuesta del firmware
Redundancia de CA	Desactivado	El CMC informa al usuario que hay pérdida de redundancia de CA.
Redundancia de suministro de energía	Desactivado	El CMC informa al usuario que hay pérdida de redundancia de suministro de energía.
Sin redundancia	Desactivado	Se disminuye la alimentación a los servidores con menor prioridad, de ser necesario.
Redundancia de CA	Activado	El CMC informa al usuario que hay pérdida de redundancia de CA. 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 desmontaje de una unidad de suministro de energía.
Redundancia de 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 desmontaje de una unidad de suministro de energía.
Sin redundancia	Activado	Se disminuye la alimentación a los servidores con menor prioridad, de ser necesario.

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 quite una unidad de suministro de energía o se quita 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 a 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 “Políticas de redundancia” en la página 344.

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

Los cambios en el modo de suministro de energía y en la política de alimentación redundancia se registran como sucesos. Los sucesos relacionados con el suministro de energía que registra 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 Tabla 9-4 muestra las entradas del SEL relacionadas con los cambios de suministros de energía.

Tabla 9-4. Sucesos del SEL para cambios de suministros de energía

Suceso de suministro de energía	Anotación del registro de sucesos del sistema (SEL)
Inserción	se declaró la presencia de suministro de energía
Extracción	se retira la declaración de presencia de suministro de energía
Se recibe entrada de CA	se retira la declaración de pérdida de entrada de suministro de energía
Entrada de CA perdida	se declaró la pérdida de entrada de suministro de energía
Se produce salida de CC	se retira la declaración de falla del suministro de energía
Salida de CC perdida	se declara la falla del suministro de energía
Se detectó una operación a 110 V no reconocida	se declaró 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 CA** o para una política de **Redundancia de suministro de energía**. La Tabla 9-5 a continuación muestra las entradas del SEL relacionadas con los cambios de política de alimentación de redundancia.

Tabla 9-5. Sucesos del SEL para cambios en el estado de redundancia de alimentación

Suceso de política de alimentación	Anotación del registro de sucesos del sistema (SEL)
Redundancia perdida	se declaró la pérdida de redundancia
Redundancia recuperada	se retiró la declaración de pérdida de redundancia

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 CA, 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 CA, el estado de redundancia será **No** y la condición general de la alimentación será **Crítica**. Esto se debe a que el sistema no puede funcionar de acuerdo con la política de redundancia configurada.



NOTA: El CMC no realiza una comprobación previa de estas condiciones cuando la política de redundancia se cambia a Redundancia de CA 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.

Configuración y administración de la alimentación

Puede utilizar las interfaces web y RACADM para administrar y configurar los controles de alimentación en el CMC. Específicamente, puede:

- Ver las asignaciones, el consumo y el estado de alimentación del chasis, los servidores y las unidades de suministro de energía.
- Configurar el Límite de alimentación de entrada del sistema y la Política de redundancia del chasis.
- Ejecutar operaciones de control de alimentación (encendido, apagado, restablecimiento del sistema, ciclo de encendido) en el chasis.

Cómo ver el estado de la condición de las unidades de suministro de energía

La página **Estado del suministro de energía** muestra el estado y las lecturas de las unidades de suministro de energía asociadas con el chasis.

Cómo utilizar la interfaz web

El estado de las unidades de suministro de energía puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado del suministro de energía**. La página **Gráficos del chasis** proporciona una descripción gráfica de todas las unidades de suministro de energía instaladas en el chasis.

Para ver el estado de la condición de todas las unidades de suministro de energía a través de **Gráficos del chasis**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Aparecerá la página **Estado del chasis**. La sección inferior de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de la condición de todas las unidades de suministro de energía. El estado de la condición de la unidad de suministro de energía se indica mediante el color del gráfico secundario de la unidad de suministro de energía:
 - Verde: la unidad de suministro de energía está presente, encendida y se está comunicando con el CMC; no hay ninguna indicación sobre condiciones adversas.
 - Ámbar: indica la falla de una unidad de suministro de energía. Consulte el registro del CMC para ver los detalles de la condición de falla.
 - Gris: aparece durante la inicialización de la unidad de suministro de energía y cuando la unidad se define en el modo de espera, durante el encendido del chasis o la inserción de la unidad de suministro de energía. La unidad está presente y apagada. No existe una indicación de una condición adversa.
- 3 Pase el cursor sobre el gráfico secundario de una unidad de suministro de energía individual y aparecerá el cuadro de texto o el consejo de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre esa unidad de suministro de energía.
- 4 El gráfico secundario de la unidad de suministro de energía tiene un hipervínculo a la página de interfaz gráfica de usuario del CMC correspondiente para proporcionar una navegación inmediata a la página **Estado del suministro de energía** de todas las unidades de suministro de energía.

Para ver el estado de las unidades de suministro de energía a través de **Estado del suministro de energía**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Suministros de energía** en el árbol del sistema. Aparece la página **Estado del suministro de energía**.

La Tabla 9-6 y la Tabla 9-7 ofrecen descripciones de la información proporcionada en la página Estado del suministro de energía.

Tabla 9-6. Suministros de energía




Elemento	Descripción	
Nombre	Muestra el nombre de la unidad de suministro de energía: PS-[n] donde [n] es el número de la unidad.	
Presentación	Indica si la unidad de suministro de energía está Presente o Ausente .	
Condición	 En buen estado	Indica que la unidad de suministro de energía está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el suministro de energía, el CMC no podrá obtener ni mostrar la condición de la unidad de suministro de energía.
	 Aviso	Indica que solamente se han emitido alertas de aviso y que se deben realizar acciones correctivas. Si no se realizan acciones correctivas, pueden producirse fallas de alimentación críticas o graves que pueden afectar la integridad del chasis.
	 Grave	Indica que se ha emitido como mínimo una alerta de falla para el suministro de energía. El estado de falla indica una falla de alimentación en el chasis y se debe realizar una acción correctiva inmediatamente .
Estado de la alimentación	Muestra el estado de la alimentación de los suministros de energía (uno de los siguientes): Inicializando, En línea, En espera, En diagnóstico, Fallido, Fuera de línea, Desconocido o Ausente .	
Capacidad	Muestra la capacidad de alimentación en vatios.	

Tabla 9-7. Estado de alimentación del sistema

Elemento	Descripción
Condición general de la alimentación	Muestra el estado de la condición (En buen estado, No crítico, Crítico, No recuperable, Otro, Desconocido) de la administración de la alimentación de todo el chasis.
Estado de alimentación del sistema	Muestra el estado de la alimentación (Encendido, Apagado, Encendiéndose, Apagándose) del chasis.
Redundancia	Muestra el estado de redundancia del suministro de energía. Los valores incluyen: No: los suministros de energía no son redundantes. Sí: hay redundancia total.

Cómo utilizar de RACADM

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

```
racadm getpminfo
```

Para obtener más información sobre **getpminfo**, incluidos los detalles de salida, consulte la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC) en el sitio web del servicio de asistencia Dell Support en support.dell.com/manuals.

Cómo ver el estado del consumo de alimentación

El CMC proporciona el consumo de alimentación de entrada real para todo el sistema en la página **Estado del consumo de alimentación**.

Cómo utilizar la interfaz web



NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Para ver el estado del consumo de alimentación por medio de la interfaz web:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3 Haga clic en **Alimentación** → **Consumo de alimentación**. Se muestra la página **Consumo de alimentación**.



NOTA: También puede ver el estado de redundancia de alimentación en **Suministros de energía** en el árbol **Sistema** → ficha **Estado**.

Cómo utilizar de RACADM

Para ver el estado del consumo de alimentación con RACADM:

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

```
racadm getpminfo
```

De la Tabla 9-8 a la Tabla 9-11 se describe la información que se muestra en la página **Consumo de alimentación**.

Tabla 9-8. Estadísticas de alimentación de tiempo real

Elemento	Descripción
Alimentación de entrada del sistema	Indica el consumo acumulado actual de alimentación de todos los módulos en el chasis medido desde la entrada de las unidades de suministro de energía. El valor de la alimentación de entrada del sistema se indica en vatios y en BTU/h.
Alimentación pico del sistema	Muestra el nivel máximo de consumo de alimentación de entrada en el sistema desde la última vez que se borró el valor. Esta propiedad le permite dar seguimiento al consumo máximo de alimentación del sistema (el chasis y los módulos) registrado durante un periodo. Haga clic en el botón Restablecer estadísticas de alimentación pico/mínima que aparece debajo de la tabla para borrar este valor. El valor de la alimentación pico del sistema se indica en vatios y en BTU/h.
Hora de inicio de la alimentación pico del sistema	Muestra la fecha y la hora registradas cuando se borró por última vez el valor de consumo de alimentación pico del sistema. La fecha y hora se muestran en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año. Este valor se restablece con el botón Restablecer estadísticas de alimentación pico/mínima y también cuando se restablece o falla el CMC.
Fecha y hora de la alimentación pico del sistema	Muestra la fecha y la hora registradas cuando se presentó el consumo de alimentación pico del sistema durante el periodo registrado. La fecha y la hora se muestran en el formato hh:mm:ss MM/DD/YYYY , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y YYYY es el año.

Tabla 9-8. Estadísticas de alimentación de tiempo real (continuación)

Elemento	Descripción
Alimentación mínima del sistema	Muestra el valor del consumo de nivel mínimo de corriente alterna en el sistema (en vatios) en el tiempo desde la última vez que el usuario borró este valor. Esta propiedad permite seguir de cerca el consumo mínimo de alimentación del sistema (chasis y módulos) registrado durante un periodo. Haga clic en el botón Restablecer estadísticas de alimentación pico/mínima que aparece debajo de la tabla para borrar este valor. El valor de la alimentación mínima del sistema se muestra en vatios y en BTU/h. Este valor se restablece con el botón Restablecer estadísticas de alimentación pico/mínima y también cuando se restablece o falla el CMC.
Hora de inicio de la alimentación mínima del sistema	Muestra la fecha y la hora registradas cuando se borró por última vez el valor de consumo mínimo de alimentación del sistema. La fecha y hora se muestran en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año. Este valor se restablece con el botón Restablecer estadísticas de alimentación pico/mínima y también cuando se restablece o falla el CMC.
Fecha y hora de la alimentación mínima del sistema	Muestra la fecha y hora registradas cuando se presentó el consumo mínimo de alimentación del sistema durante el periodo registrado. El formato de la fecha y hora es el mismo que el descrito para Fecha y hora de la alimentación pico del sistema .
Alimentación del sistema en inactividad	Muestra el consumo estimado de alimentación del chasis cuando está en estado de inactividad. El estado de inactividad se define como el estado del chasis mientras está encendido y todos los módulos consumen energía mientras está en estado de inactividad. <i>Este es un valor calculado y no obtenido por medición.</i> Se calcula como la alimentación acumulada asignada a los componentes de la infraestructura del chasis (módulos de E/S, ventiladores, iKVM, controladoras iDRAC y LCD del panel anterior) y el requerimiento mínimo de alimentación de todos los servidores a los que se asignó alimentación y que se encuentran encendidos. El valor de la alimentación del sistema en inactividad se indica en vatios y en BTU/h.

Tabla 9-8. Estadísticas de alimentación de tiempo real (continuación)

Elemento	Descripción
Alimentación potencial del sistema	Muestra el consumo estimado de alimentación del chasis cuando funciona a la máxima potencia. El consumo máximo de alimentación se define como el estado del chasis cuando está encendido y todos los módulos consumen alimentación máxima. <i>Este es un valor estimado derivado del consumo de alimentación acumulado histórico de la configuración del sistema y no se trata de un valor obtenido por medición.</i> Se calcula como la alimentación acumulada asignada a los componentes de la infraestructura del chasis (módulos de E/S, ventiladores, iKVM, controladoras iDRAC y LCD del panel anterior) y el requerimiento máximo de alimentación de todos los servidores a los que se asignó alimentación y que se encuentran encendidos. El valor de la alimentación potencial del sistema se indica en vatios y en BTU/h.
Lectura de la corriente de entrada del sistema	Muestra el consumo de corriente de entrada total del chasis con base en la suma del consumo de corriente de entrada de cada uno de los módulos de las unidades de suministro de energía individuales del chasis. El valor de la lectura de la corriente de entrada del sistema se muestra en amperios.

Tabla 9-9. Estado de las estadísticas de energía en tiempo real

Elemento	Descripción
Consumo de energía del sistema	Indica el consumo acumulado actual de energía de todos los módulos en el chasis medido desde la entrada de los suministros de energía. El valor se muestra en kilovatios hora y es un valor acumulado.
Hora de inicio del consumo de energía del sistema	Muestra la fecha y la hora registradas cuando se borró por última vez el valor de consumo de energía del sistema y comenzó el nuevo ciclo de mediciones. La fecha y hora se muestran en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año. Este valor se restablece con el botón Restablecer estadísticas de energía , pero persistirá a lo largo de las operaciones de restablecimiento o de transferencia de funciones ante fallas del CMC.

Tabla 9-9. Estado de las estadísticas de energía en tiempo real (continuación)

Elemento	Descripción
Fecha y hora del consumo de energía del sistema	Muestra la fecha y hora cuando se calculó el consumo de energía del sistema para mostrarlo. La fecha y hora se muestran en el formato hh:mm:ss MM/DD/AAAA , donde hh son las horas (0-24), mm son los minutos (00-60), ss son los segundos (00-60), MM es el mes (1-12), DD es el día (1-31) y AAAA es el año.

Tabla 9-10. Estado de alimentación del sistema

Elemento	Descripción
Condición general de la alimentación	Indica la condición del subsistema de alimentación del chasis: <ul style="list-style-type: none"> • El icono de marca verde significa En buen estado • El icono del signo de exclamación amarillo significa No crítico • El icono de la X roja significa Crítico
Estado de alimentación del sistema	Muestra el estado de la alimentación (Encendido, Apagado, Encendiéndose, Apagándose) del chasis.
Redundancia	Muestra el estado de redundancia. Los valores válidos son: No : las unidades de suministro de energía no son redundantes Sí : hay redundancia total

Tabla 9-11. Módulos del servidor

Elemento	Descripción
Ranura	Muestra la ubicación del módulo del servidor. La Ranura es un número en secuencia (1 a 16) que identifica el módulo de servidor por su ubicación dentro del chasis.
Nombre	Muestra el nombre del servidor. El usuario puede redefinir el nombre del servidor.
Presentación	Indica si el servidor está presente en la ranura (Sí o No). Si este campo muestra la Extensión de N.º (donde el N.º será de 1 a 8), entonces el número que lo siga será la ranura principal de un servidor con múltiples ranuras.

Tabla 9-11. Módulos del servidor (continuación)

Elemento	Descripción
Real (CA)	Medición en tiempo real del consumo de alimentación real del servidor. La medición se muestra en vatios de CA.
Hora de inicio de la alimentación acumulada	Medición en tiempo real de la alimentación acumulada que el servidor ha consumido desde que se mostró la hora en el campo Hora de inicio . La medición se presenta en kilovatios hora (kWh).
Fecha y hora del consumo pico	Muestra la alimentación pico que el servidor consumió en cierto momento. La hora en la que ocurrió el consumo de alimentación pico se registra en el campo Fecha y hora . La medición se muestra en vatios.

Cómo ver el estado del presupuesto de alimentación

El CMC proporciona descripciones generales del estado de alimentación del subsistema de energía en la página **Estado de presupuesto de alimentación**.

Cómo utilizar la interfaz web



NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Para ver el estado de presupuesto de alimentación por medio de la interfaz web:

- 1** Inicie sesión en la interfaz web del CMC.
- 2** Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3** Haga clic en **Alimentación** → **Estado del presupuesto**.
Se muestra la página **Estado de presupuesto de alimentación**.

De la Tabla 9-12 a la Tabla 9-15 se describe la información que se muestra en la página **Estado de presupuesto de alimentación**.

Consulte la sección “Configuración del presupuesto y la redundancia de alimentación” en la página 369 para obtener información acerca de cómo configurar los valores para esta información.

Cómo utilizar de 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 la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Tabla 9-12. Configuración de la política de alimentación del sistema

Elemento	Descripción
Límite de alimentación de entrada del sistema	<p>Indica el límite máximo de consumo de alimentación definido por el usuario para todo el sistema (chasis, CMC, servidores, módulos de E/S, unidades de suministro de energía, iKVM y ventiladores).</p> <p>El CMC aplicará este límite regulando la asignación de alimentación a los servidores o apagando los módulos de los servidores de menor prioridad. El valor del límite de alimentación de entrada del sistema se muestra en vatios, BTU/h y porcentajes.</p> <p>Si el consumo de energía del chasis excede el Límite de alimentación de entrada del sistema, el rendimiento de los servidores con menor prioridad se reducirá hasta que el consumo total de energía sea menor al límite.</p> <p>En los casos en los que se establezcan servidores con la misma prioridad, la selección del servidor para la reducción de la alimentación, o para la acción de apagado, se basa en el orden del número de ranura del servidor. Por ejemplo, el servidor en la ranura 1 se selecciona primero y el servidor en la ranura 16 se selecciona al último.</p>

Tabla 9-12. Configuración de la política de alimentación del sistema (continuación)

Elemento	Descripción
Política de redundancia	<p>Muestra la configuración de redundancia actual: Redundancia de CA, Redundancia de suministro de energía y Sin redundancia.</p> <p>Redundancia de CA: la carga de la entrada de potencia se reparte de manera equilibrada entre todas las unidades de suministro de energía. La mitad de ellas deben estar cableadas a una red de CA y la otra mitad a la otra red eléctrica. Cuando el sistema funciona de manera óptima en el modo Redundancia de CA, la carga de la alimentación se distribuye entre todos los suministros activos. En caso de una falla de la red eléctrica, las unidades de suministro de energía en la red de CA que está funcionando toman el control sin que haya interrupciones.</p> <p>Redundancia de suministro de energía: la capacidad de la unidad de suministro de energía con la clasificación más alta del chasis se mantiene en reserva para garantizar que una falla en cualquiera de las unidades de suministro de energía no ocasione que los módulos de servidor o el chasis se apaguen.</p> <p>Existe la posibilidad de que la redundancia de suministro de energía no utilice las seis unidades de suministro de energía, ya que utiliza las unidades suficientes para garantizar que si falla alguna, las restantes puedan continuar suministrando energía al chasis. Las demás unidades de suministro de energía pueden ponerse en el modo En espera si DPSE está activada.</p> <p>Sin redundancia: la energía de todas las unidades de suministro de energía activas es suficiente para alimentar a todo el chasis, lo que incluye el chasis, los servidores, los módulos de E/S, iKVM y CMC. Las unidades de suministro de energía restantes pueden ponerse en el modo En espera si DPSE está activada.</p> <p>⚠ PRECAUCIÓN: El modo Sin redundancia utiliza solo la cantidad mínima requerida de unidades de suministro de energía al mismo tiempo, sin respaldo. La falla de una de las unidades de suministro de energía en uso puede ocasionar que los módulos de servidor pierdan alimentación y datos.</p>
Conexión dinámica del suministro de energía	<p>Muestra si la Conexión dinámica del suministro de energía está activada o desactivada. La activación de esta función permite al CMC poner las unidades de suministro de energía poco utilizadas en modo de espera, dependiendo de la política de redundancia establecida y de los requisitos de alimentación del sistema. Al poner las unidades de suministro de energía subutilizadas en modo de espera, se incrementa la utilización y la eficacia de las unidades de suministro de energía en línea, lo que ahorra energía.</p>

Tabla 9-13. Presupuesto de alimentación

Elemento	Descripción
Capacidad máx. de alimentación de entrada del sistema	Máxima alimentación de entrada que los suministros de energía disponibles pueden proporcionar al sistema (en vatios).
Reserva de redundancia de entrada	<p>Muestra la cantidad de alimentación redundante (en vatios) en reserva que se puede utilizar en caso de falla de la red de CA o de una unidad de suministro de energía.</p> <p>Cuando el chasis se configura para funcionar en modo de Redundancia de CA, la Reserva de redundancia de entrada es la cantidad de alimentación de reserva que se puede utilizar en caso de falla de la red de CA.</p> <p>Cuando el chasis se configura para funcionar en modo de Redundancia suministro de energía, la Reserva de redundancia de entrada es la cantidad de alimentación de reserva que se puede utilizar en caso de falla de la unidad de suministro de energía.</p>
Alimentación de entrada asignada a los servidores	Muestra la alimentación de entrada acumulada (en vatios) que el CMC asigna a los servidores con base en su configuración.
Alimentación de entrada asignada a la infraestructura de chasis	Muestra la energía de entrada acumulada (en vatios) que el CMC asigna a la infraestructura del chasis (ventiladores, módulos de E/S, iKVM, CMC, CMC en espera e iDRAC en servidores).
Alimentación total de entrada disponible para asignar	Muestra la alimentación total del chasis, expresada en vatios, que aún está disponible para asignar.
Capacidad de alimentación de entrada en espera	<p>Muestra la cantidad de alimentación de entrada en espera (en vatios) disponible en el caso de una falla en el suministro de energía o un desmonte del suministro de energía del sistema. Es posible que este campo muestre lecturas cuando el sistema tenga varios suministros de energía y la conexión dinámica del suministro de energía esté activada.</p> <p>NOTA: Es posible ver una unidad de suministro de energía modo de espera pero no contribuir al valor de Capacidad de alimentación de entrada en espera. En este caso, los vatios de esta unidad de suministro de energía contribuyen al valor Alimentación total de entrada disponible para asignar.</p>

Tabla 9-14. Módulos del servidor

Elemento	Descripción
Ranura	Muestra la ubicación del módulo del servidor. La Ranura es un número en secuencia (1 a 16) que identifica el módulo de servidor por su ubicación dentro del chasis.
Nombre	Muestra el nombre del servidor. El nombre del servidor lo define el usuario.
Tipo	Muestra el tipo del servidor.
Prioridad	<p>Muestra el nivel de prioridad asignado a la ranura del servidor en el chasis para elaborar el presupuesto de alimentación. El CMC utiliza este valor en sus cálculos cuando la alimentación se debe reducir o reasignar dependiendo de los límites de la alimentación definidos por el usuario o debido a fallas del suministro de energía o de la red eléctrica.</p> <p>Niveles de prioridad: 1 (la mayor) a 9 (la menor)</p> <p>Valor predeterminado: 1</p> <p>NOTA: El nivel de prioridad de la ranura del servidor está asociado con la ranura del servidor, no con el servidor insertado en la ranura. Si un servidor se mueve a una ranura diferente en el chasis o a otro chasis, la prioridad asociada anteriormente con la nueva ranura determina la prioridad del servidor reubicado.</p>
Estado de la alimentación	<p>Muestra el estado de la alimentación del servidor:</p> <ul style="list-style-type: none"> • N/A: el CMC no ha determinado el estado de la alimentación del servidor. • Apagado: el servidor o el chasis están apagados. • Encendido: tanto el chasis como el servidor están encendidos. • Encendiendo: estado temporal entre apagado y encendido. Cuando se complete el ciclo de encendido, el estado de la alimentación cambiará a Encendido. • Apagando: estado temporal entre Encendido y Apagado. Cuando se complete el ciclo de apagado, el estado de la alimentación cambiará a Apagado.
Asignación de presupuesto: real	<p>Muestra la cantidad asignada de presupuesto de alimentación para el módulo de servidor.</p> <ul style="list-style-type: none"> • Real: asignación de presupuesto de alimentación actual de cada servidor.

Tabla 9-15. Suministros de energía del chasis

Elemento	Descripción
Nombre	Muestra el nombre de la unidad de suministro de energía en el formato PS- <i>n</i> , donde <i>n</i> es el número de la unidad de suministro de energía.
Estado de la alimentación	Muestra el estado de la alimentación de la unidad de suministro de energía: Inicializando , En línea , En espera , En diagnóstico , Fallido , Desconocido o Ausente (faltante).
Voltios de entrada	Muestra el voltaje de entrada actual del suministro de energía.
Corriente de entrada	Muestra la corriente de entrada actual del suministro de energía.
Potencia nominal de salida	Muestra la potencia nominal máxima de salida del suministro de energía.

Configuración del presupuesto y la redundancia de alimentación

El servicio de administración de la alimentación del CMC optimiza el consumo de alimentación para todo el chasis (el chasis, los servidores, los módulos de E/S, el iKVM, el CMC y las unidades de suministro de energía) y reasigna la alimentación a distintos módulos en función de la demanda.

Cómo utilizar la interfaz web



NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Para configurar el presupuesto de alimentación por medio de la interfaz web:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3 Haga clic en **Alimentación** → **Configuración**.
Aparecerá la página **Configuración de redundancia/presupuesto**.
- 4 Establezca cualquiera o todas las propiedades descritas en la Tabla 9-16 según sus necesidades.
- 5 Haga clic en **Aplicar** para guardar los cambios.

Para actualizar el contenido de la página **Configuración de redundancia/presupuesto**, haga clic en **Actualizar**. Para imprimir el contenido, haga clic en **Imprimir**.

Tabla 9-16. Propiedades configurables del presupuesto/la redundancia de alimentación

Elemento	Descripción
Límite de alimentación de entrada del sistema	<p data-bbox="351 347 956 579">El límite de alimentación de entrada del sistema es la alimentación máxima de CA que el sistema puede asignar a los servidores y a la infraestructura del chasis. Puede ser configurada por el usuario con cualquier valor que exceda la alimentación mínima necesaria para los servidores que se encienden y para la infraestructura del chasis. Si se configura un valor menor a la alimentación mínima necesaria para los servidores y la infraestructura del chasis, este no servirá.</p> <p data-bbox="351 595 956 767">La alimentación asignada a los servidores y a la infraestructura del chasis puede encontrarse en la interfaz del usuario, en la página de estado Descripción general del chasis→ Alimentación → Presupuesto de alimentación en la sección Presupuesto de alimentación o bien mediante el comando la utilidad de CLI RACADM (<code>racadm getpbinfo</code>).</p> <p data-bbox="351 783 956 956">Los usuarios pueden apagar uno o más servidores para disminuir la asignación actual de alimentación e intentar configurar otra vez un valor menor para el Límite de alimentación de entrada del sistema (si así se desea) o simplemente para configurar el límite antes de encender los servidores.</p> <p data-bbox="351 971 956 1083">Para cambiar esta configuración, se puede introducir un valor en cualquiera de las unidades. La interfaz asegura que el campo de unidades que se cambió por última vez será el valor que se envíe cuando se apliquen los cambios.</p> <p data-bbox="351 1099 956 1182">NOTA: Consulte la herramienta Datacenter Capacity Planner (DCCP) en www.dell.com/calc para obtener información sobre la planificación de la capacidad.</p> <p data-bbox="351 1198 956 1396">NOTA: Cuando los cambios de los valores se especifican en vatios, el valor enviado reflejará exactamente lo que se aplica en realidad. Sin embargo, cuando los cambios se envían en BTU/h o en porcentajes, el valor enviado no reflejará exactamente lo que se aplica en realidad. Esto se debe a que las unidades son convertidas a vatios y después se aplican; y es posible que la conversión sea susceptible a errores de redondeo.</p>

Tabla 9-16. Propiedades configurables del presupuesto/la redundancia de alimentación (continuación)

Elemento	Descripción
Política de redundancia	<p data-bbox="389 312 956 363">Esta opción le permitirá seleccionar una de las siguientes opciones:</p> <ul data-bbox="398 376 997 485" style="list-style-type: none"> <li data-bbox="398 376 997 485">• Sin redundancia: la alimentación de los suministros de energía se utiliza para todo el chasis, lo que incluye el chasis, los servidores, los módulos de E/S, el iKVM y el CMC. No deben dejarse suministros de energía en reserva. <p data-bbox="389 497 997 740">NOTA: El modo Sin redundancia utiliza solo la cantidad mínima requerida de suministros de energía al mismo tiempo. Si está instalada la cantidad requerida de unidades de suministro de energía, no habrá ninguna unidad de respaldo disponible. La falla de uno de los tres suministros de energía podría provocar que los servidores pierdan alimentación y/o datos. Si hay más unidades de suministro de energía que las requeridas, las unidades adicionales pueden ponerse en el modo En espera para mejorar la eficiencia energética si DPSE está activada.</p> <ul data-bbox="398 753 997 893" style="list-style-type: none"> <li data-bbox="398 753 997 893">• Redundancia de suministro de energía: la capacidad del suministro de energía con la clasificación más alta en el chasis se mantiene en reserva, para asegurar que una falla de cualquier suministro de energía no ocasione que los módulos de servidor o el chasis se apaguen (repuesto dinámico). <p data-bbox="418 906 997 1046">En el modo Redundancia de suministro de energía no es necesario utilizar todos los suministros de energía instalados. Cualquier suministro de energía adicional (si está presente) puede colocarse en el modo En espera para mejorar la eficiencia energética cuando DPSE está activada.</p> <p data-bbox="418 1043 997 1123">Redundancia de suministro de energía evita que los módulos de servidor se enciendan si el consumo de la alimentación del chasis excede la potencia nominal.</p> <p data-bbox="418 1126 997 1235">La falla de dos suministros de energía podría ocasionar que se apaguen todos o algunos de los módulos del servidor en el chasis. El rendimiento del módulo del servidor no se degrada en este modo.</p> <ul data-bbox="398 1248 997 1436" style="list-style-type: none"> <li data-bbox="398 1248 997 1436">• Redundancia de CA: este modo divide la mitad de las unidades de suministro de energía en dos redes eléctricas (por ejemplo, las unidades 1 a 3 conforman la red eléctrica 1 y las unidades 4 a 6 conforman la red eléctrica 2). Si falla una unidad de suministro de energía o se pierde la alimentación de corriente alterna en una red eléctrica, el estado de redundancia se informa como perdido.

Tabla 9-16. Propiedades configurables del presupuesto/la redundancia de alimentación (continuación)

Elemento	Descripción
Rendimiento del sistema sobre redundancia de alimentación	<p>Cuando está activada, esta opción favorece el rendimiento y el encendido del servidor ante el mantenimiento de la redundancia de alimentación. Para obtener más información acerca de esta función, ver “Rendimiento del sistema sobre redundancia de alimentación” en la página 348.</p>
Activar conexión dinámica del suministro de energía	<p>Al seleccionar esta opción se activa la administración dinámica de la alimentación. En el modo Conexión dinámica, los suministros de energía están Encendidos (en línea) o Apagados (en espera) en función del consumo de alimentación, lo que optimiza el consumo de alimentación de todo el chasis.</p> <p>Por ejemplo, usted tiene presupuesto de alimentación de 5000 vatios, la política de redundancia está configurada en modo de redundancia de CA, y cuenta con seis unidades de suministro de energía. El CMC determina que cuatro unidades de suministro de energía pueden administrar la redundancia de CA mientras que las otras dos permanecen en modo de espera. Si hacen falta 2000 W de potencia adicionales para servidores recién instalados o se debe mejorar la eficiencia energética de la configuración del sistema existente, se conectarán las dos unidades de suministro de energía en espera.</p>
Desactivar botón de encendido del chasis	<p>Al seleccionar esta opción se desactiva el botón de encendido del chasis. Si se selecciona la casilla de verificación y se intenta cambiar el estado de la alimentación del chasis presionando el botón de encendido, la acción será ignorada.</p>
Permitir operación a 110 V CA	<p>Al seleccionar esta opción, se permitirá el funcionamiento normal si cualquier unidad de suministro de energía se conecta a una entrada de 110 V CA. Para obtener más información, ver “Operación de unidades de suministro de energía de 110 V” en la página 348.</p>
Modo de conservación máxima	<p>Al seleccionar esta opción, se introduce de inmediato al modo de conservación máxima de la alimentación. Para obtener más información, ver “Conservación de la energía y modo de conservación máxima” en la página 346.</p>

Cómo utilizar de RACADM

Para activar la redundancia y establecer la política de redundancia:



NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

- 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 <valor>
```

donde <valor> es 0 (Sin redundancia), 1 (Redundancia de CA), 2 (Redundancia de suministro de energía). El valor predeterminado es 0.

Por ejemplo, el siguiente comando:

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

establece la política de redundancia en 1.

- Para activar o desactivar la conexión dinámica de las unidades de suministro de energía, escriba:

```
racadm config -g cfgChassisPower -o  
cfgChassisDynamicPSUEngagementEnable <valor>
```

donde <valor> es 0 (desactivar), 1 (activar). El valor predeterminado es 0.

Por ejemplo, el siguiente comando:

```
racadm config -g cfgChassisPower -o  
cfgChassisDynamicPSUEngagementEnable 0
```

desactiva la conexión dinámica de las unidades de suministro de energía.

Para obtener más información acerca de los comandos RACADM para la alimentación del chasis, consulte las secciones **config**, **getconfig**, **getpbinfo** y **cfgChassisPower** de la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC).

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 asigna a un servidor está vinculada a la ranura y no al servidor. Si traslada el servidor a una nueva ranura, debe reconfigurar la prioridad de la ubicación de la nueva ranura.



NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Cómo utilizar la interfaz web

Para asignar niveles de prioridad por medio de la interfaz web del CMC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de servidores** en el árbol del sistema. Aparece la página **Estado de los servidores**.
- 3 Haga clic en **Alimentación** → **Prioridad de servidores**. Aparece la página **Prioridad de servidores**, en la que se muestra una lista de todos los servidores del chasis.
- 4 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.
- 5 Haga clic en **Aplicar** para guardar los cambios.

Cómo utilizar de 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> (1 a 16) se refiere a la ubicación del servidor y <nivel de prioridad> es un valor entre 1 y 9.

Por ejemplo, el siguiente comando:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

Establece el nivel de prioridad en 1 para el servidor en la ranura 5.

Cómo establecer el presupuesto de alimentación



NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Cómo utilizar la interfaz web

Para establecer el presupuesto de alimentación por medio de la interfaz web del CMC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Descripción general del chasis** en el árbol del sistema. Aparecerá la página **Condición del chasis**.
- 3 Haga clic en la ficha **Alimentación**. Aparece la página **Estado del consumo de alimentación**.
- 4 Haga clic en la subficha **Configuración**. Aparece la página **Configuración de redundancia/presupuesto**.
- 5 Escriba un valor de presupuesto de hasta 16685 vatios en el campo de texto **Límite de alimentación de entrada del sistema**.



NOTA: El presupuesto de alimentación se limita al máximo de cualquier grupo de tres unidades de suministro de energía que sea el más débil. Si intenta establecer un presupuesto de alimentación de CA que exceda este valor, CMC mostrará un mensaje de falla.



NOTA: Cuando los cambios de los valores se especifican en vatios, el valor enviado reflejará exactamente lo que se aplica en realidad. Sin embargo, cuando los cambios se envían en unidades BTU/h o porcentajes, es posible que el valor enviado no refleje exactamente lo que en realidad se aplica. Esto se debe a que las unidades son convertidas a vatios y después se aplican; y es posible que la conversión sea susceptible a errores de redondeo.

- 6 Haga clic en **Aplicar** para guardar los cambios.

Cómo utilizar de RACADM

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

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

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:

```
racadm config -g cfgChassisPower -o  
cfgChassisPowerCap 5400
```

establece el presupuesto de alimentación máximo en 5.400 vatios.



NOTA: El presupuesto de alimentación está limitado a 16685 vatios. Si intenta definir un valor de presupuesto máximo de alimentación de CA que sobrepase la capacidad de alimentación del chasis, el CMC mostrará un mensaje de falla.

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 **Límite de alimentación de entrada del sistema**. Por ejemplo, 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 **Límite de alimentación de entrada del sistema** configurable (ver “Cómo establecer el presupuesto de alimentación” en la página 375).
- Se produce una falla de alimentación en una configuración sin redundancia

Para obtener información sobre la asignación de niveles de prioridad a los servidores, ver “Ejecución de operaciones de control de alimentación en el chasis” en la página 377.

Ejecución de operaciones de control de alimentación en el chasis



NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.





NOTA: Las operaciones de control de alimentación afectan a todo el chasis. Para las operaciones de control de alimentación en un módulo de E/S, ver “Ejecución de las operaciones de control de alimentación en un módulo de E/S” en la página 379. Para las operaciones de control de alimentación en servidores, ver “Ejecución de operaciones de control de alimentación en un servidor” en la página 380.

El CMC le permite realizar de manera remota varias acciones de administración de la alimentación, como 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).


Cómo utilizar la interfaz web

Para ejecutar operaciones de control de alimentación en el chasis por medio de la interfaz web del CMC:


- 1 Inicie sesión en la interfaz web del CMC.
 - 2 Seleccione **Descripción general del chasis** en el árbol del sistema.
 - 3 Haga clic en la ficha **Alimentación**.
Aparecerá la página **Estado del consumo de alimentación**.
 - 4 Haga clic en la subficha **Control**. Aparecerá la página **Control de alimentación del chasis**.
 - 5 Haga clic en los botones de radio correspondientes para seleccionar una de las siguientes **operaciones de control de alimentación**:
 - **Encender el sistema:** Enciende la alimentación del chasis (equivale a presionar el botón de encendido cuando la alimentación del chasis está **Apagada**). Esta opción está desactivada si el chasis ya está **Encendido**.
-  **NOTA:** Esta opción enciende el chasis y otros subsistemas (el iDRAC en los servidores, los módulos de E/S y el iKVM). Los servidores no se encienden.
- **Apagar el sistema:** apaga la alimentación del chasis. Esta acción se desactivará si el chasis ya está **Apagado**.

 **NOTA:** Esta acción apaga el chasis (chasis, servidores, módulos de E/S, iKVM y suministros de energía). Los CMC permanecen encendidos, pero en un estado de espera virtual; una unidad de suministro de energía y ventiladores enfrían los CMC en este estado. El suministro de energía también proporciona alimentación a los ventiladores que funcionan a baja velocidad.

- **Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía):** apaga el sistema y después lo reinicia (reinicio mediante suministro de energía). Esta acción se desactivará si el chasis ya está **Apagado**.

 **NOTA:** Esta acción apaga y después reinicia el chasis completo (chasis, servidores configurados para estar siempre encendidos, módulos de E/S, iKVM y suministros de energía).

- **Restablecer el CMC:** restablece el CMC sin apagarlo (reinicio mediante sistema operativo). Esta opción se desactiva si el CMC ya está apagado.

 **NOTA:** Esta acción solo restablece el CMC. No se afecta a ningún otro componente.

- **Apagado no ordenado:** esta acción fuerza un apagado no ordenado de todo el chasis (chasis, servidores, módulos de E/S, iKVM y suministros de energía). No intenta cerrar de forma ordenada el sistema operativo de los servidores antes de apagarlos.

6 Haga clic en **Aplicar**. Aparece un cuadro de diálogo que solicita confirmación.

7 Haga clic en **Aceptar** para realizar la acción de administración de la alimentación (por ejemplo, hacer que se reinicie el sistema).

Cómo utilizar de RACADM

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

```
racadm chassisaction -m chassis <acción>
```

donde <acción> es powerup, powerdown, powercycle, nongraceshutdown o reset.

Ejecución de las operaciones de control de alimentación en un módulo de E/S

Usted puede 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 alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Cómo utilizar la interfaz web

Para ejecutar operaciones de control de alimentación en un módulo de E/S por medio de la interfaz web del CMC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Descripción general de módulos de E/S**.
Aparecerá la página **Estado de los módulos de E/S**.
- 3 Haga clic en la ficha **Alimentación**.
Aparecerá la página **Control de alimentación**.
- 4 Seleccione la operación que desea ejecutar (**reinicio** o **ciclo de encendido**) en el menú desplegable que se encuentra junto al módulo de E/S en la lista.
- 5 Haga clic en **Aplicar**.
Aparece un cuadro de diálogo que solicita confirmación.
- 6 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).

Cómo utilizar de 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 de 1 a 6 y especifica el módulo de E/S (A1, A2, B1, B2, C1, C2), y <acción> indica la operación que desea ejecutar:

```
powercycle o reset.
```

Ejecución de operaciones de control de alimentación en un servidor




NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

El CMC le permite realizar de manera remota varias acciones de administración de la alimentación, por ejemplo, un apagado ordenado en un servidor individual del chasis.

Cómo utilizar la interfaz web

Para operaciones de control de alimentación en un servidor por medio de la interfaz web:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Expanda **Descripción general de servidores** en el árbol del sistema y después seleccione el servidor en el que desee ejecutar una operación de control de alimentación. Aparece la página **Estado del servidor**.
- 3 Haga clic en la ficha **Alimentación**.
Aparece la página **Administración de la alimentación del servidor**.
- 4 **Estado de alimentación** muestra el estado de alimentación del servidor (uno de los siguientes):
 - **N/A:** el CMC no ha determinado aún el estado de la alimentación del servidor.
 - **Apagado:** el servidor o el chasis están apagados.
 - **Encendido:** tanto el chasis como el servidor están encendidos.
 - **Encendiendo:** estado temporal entre Apagado y Encendido. Cuando la acción finalice satisfactoriamente, el **Estado de la alimentación** estará **Encendido**.
 - **Apagando:** estado temporal entre Encendido y Apagado. Cuando la acción finalice satisfactoriamente, el **Estado de la alimentación** estará **Apagado**.

- 5 Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en su botón de radio:
- **Encender el servidor:** enciende el servidor (equivale a presionar el botón de encendido cuando el servidor está apagado). Esta acción se desactivará si el servidor ya está encendido.
 - **Apagar el servidor:** apaga el servidor (equivale a presionar el botón de encendido cuando el servidor está encendido).
 - **Apagado ordenado:** apaga y después reinicia el servidor.
 - **Restablecer el sistema (reinicio mediante sistema operativo):** Reinicia el servidor sin apagarlo. Esta opción se desactiva cuando el servidor ya está apagado.
 - **Ciclo de encendido del servidor (reinicio mediante suministro de energía):** apaga el servidor y después lo reinicia. Esta opción se desactiva cuando el servidor ya está apagado.
- 6 Haga clic en **Aplicar**. Aparece un cuadro de diálogo que solicita confirmación.
- 7 Haga clic en **Aceptar** para realizar la acción de administración de alimentación (por ejemplo, hacer que el servidor se restablezca).
-  **NOTA:** Todas las operaciones de control de alimentación pueden ejecutarse en varios servidores desde la página **Servidores**→ **Alimentación**→ **Control**.

Cómo utilizar de RACADM

Para ejecutar operaciones de control de alimentación en un servidor mediante RACADM:

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

```
racadm serveraction -m <módulo> <acción>
```

donde <modulo> especifica el servidor por su número de ranura (servidor 1 a 16) en el chasis y <acción> indica la operación que desea ejecutar: `powerup`, `powerdown`, `powercycle`, `graceshutdown` o `hardreset`.

Operación a 110 V

Algunos modelos de suministros de energía (unidades de suministro de energía) son capaces de funcionar con corrientes de 220 V o 110 V. La energía de 110 V puede ofrecer capacidad limitada, y es por eso que cuando se detecta una conexión de 110 V el chasis no acepta las solicitudes adicionales de energía del servidor sino hasta que el usuario confirma la operación a 110 V mediante el cambio de la propiedad de configuración de alimentación. El usuario debe verificar que el circuito de 110 V que está en uso pueda proporcionar la alimentación requerida para la configuración del chasis antes de confirmar la operación. Después de confirmarla, el chasis aceptará todas las solicitudes de alimentación del servidor correspondiente que se realicen en el futuro y utilizará toda la capacidad de suministro de energía disponible.

El usuario puede restablecer la confirmación de 110 V en todo momento a través de la interfaz gráfica de usuario o de RACADM después de la instalación inicial. Las anotaciones de suministros de energía se registran en el registro SEL cuando se detectan o se quitan suministros de 110 V. También se registran anotaciones cuando la operación es confirmada o no confirmada por el usuario.

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. El icono de aviso se muestra en la página principal de la interfaz gráfica de usuario durante este estado No crítico.

No se admiten operaciones combinadas de 110 V y 220 V. Si 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.

Administración de la alimentación externa

La administración de la alimentación del CMC se puede controlar con la “Consola de medición, mitigación y administración de la alimentación” (PM3). Para obtener más información, consulte la Guía del usuario de la PM3.

Si está activada la administración de la alimentación externa, la PM3 administra lo siguiente:

- Alimentación del servidor en servidores de 12.º generación
- Alimentación del servidor en servidores de 12.º 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 servidor sobre redundancia de alimentación
- Conexión dinámica del suministro de energía
- Alimentación del servidor en servidores de 11.º generación y anteriores

Entonces, la PM3 administra la priorización y la alimentación de los servidores blade de 12.º 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.

Cómo utilizar la interfaz web

Para activar la administración externa de la PM3:

- 1** Inicie sesión en el chasis con privilegios de **Administrador de configuración del chasis**.
- 2** Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3** Haga clic en Alimentación→ Configuración.
Se muestra la página Budget/Redundancy Configuration (Configuración de la asignación de energía/redundancia de alimentación).
- 4** Establezca el **Modo de administración de la alimentación basada en servidor**.
- 5** Haga clic en Aplicar.

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 12.º 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 del servidor compatible, 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 gestiona todos los demás límites de capacidad de alimentación.

Para desactivar la administración de la alimentación externa:

- 1 Inicie sesión en el chasis con privilegios de **Administrador de configuración del chasis**.
- 2 Seleccione **Descripción general del chasis** en el árbol del sistema.
- 3 Haga clic en **Alimentación** → **Configuración**.
Se muestra la página **Budget/Redundancy Configuration** (Configuración de redundancia de alimentación/consumo máximo).
- 4 Anule la selección del **Modo de administración de la alimentación basada en servidor**.
- 5 Haga clic en **Aplicar**.

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.

Cómo utilizar de RACADM

Abra una consola de texto de serie/Telnet/SSH en el CMC con privilegios de **Administrador de configuración del chasis**.

Para activar la administración remota de la alimentación con la 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
```


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. Consulte el **registro del CMC** para conocer la configuración anterior y restaurar el valor manualmente.

Solución de problemas

Para obtener información sobre la solución de problemas de suministros de energía y problemas relacionados con la alimentación, consulte la sección “Solución de problemas y recuperación” en la página 429.

Uso del módulo iKVM

Descripción general

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.

Interfaz de usuario del iKVM

El iKVM utiliza la interfaz gráfica de usuario OSCAR (On Screen Configuration and Reporting), que se activa mediante una tecla de acceso rápido. 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.

Sólo se permite una sesión de iKVM por chasis.

Security

La interfaz de usuario OSCAR permite proteger el sistema con una contraseña de protector de pantalla. Después de un período definido por el usuario, se inicia el modo de protección de pantalla y se prohíbe el acceso mientras no se introduzca la contraseña adecuada para reactivar OSCAR.

Exploración

OSCAR le permite seleccionar una lista de servidores, que aparecen en el orden seleccionado mientras OSCAR se encuentra en el modo de exploración.

Identificación de servidores

El CMC asigna nombres de ranuras a todos los servidores del chasis. Si bien el usuario puede asignar nombres a los servidores por medio de la interfaz OSCAR desde una conexión en nivel, los nombres asignados por el CMC tienen prioridad, por lo que los nombres nuevos asignados mediante OSCAR se sobrescribirán.

El CMC le asigna un nombre exclusivo a cada ranura para identificarla. Para cambiar los nombres de las ranuras con la interfaz web del CMC, consulte “Edición de los nombres de ranuras”. Para cambiar el nombre de una ranura mediante RACADM, consulte la sección **setslotname en la *RACADM Command Line Reference Guide for iDRAC7 and CMC*** (Guía de referencia de la línea de comandos RACADM de 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 módulo 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.

Capacidad de actualización

Es posible actualizar el firmware del iKVM por medio de la interfaz web del CMC o el comando RACADM **fwupdate**. Para obtener más información, consulte “Administración del iKVM desde el CMC” en la página 406.

Interfaces de conexión física

Puede conectarse a un servidor o a la consola CLI del CMC a través del módulo iKVM desde el panel anterior 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 anterior del chasis están específicamente diseñados para el iKVM, que es opcional. Si no se tiene el iKVM, no podrán utilizarse los puertos del panel anterior.

Prioridades de las conexiones del iKVM

Sólo se permite una conexión de iKVM a la vez. El iKVM asigna un orden de prioridad a cada tipo de conexión, de manera que cuando existan varias solo una esté disponible y las demás queden desactivadas.

El orden de prioridad de las conexiones del iKVM es el siguiente:

- 1 Panel anterior
- 2 ACI
- 3 Panel posterior

Por ejemplo, si existen conexiones de iKVM en el panel anterior y la ACI, la conexión del panel anterior permanecerá activa y la otra quedará desactivada. Si existen conexiones del panel posterior y la ACI, las conexiones de la ACI tendrán prioridad.

Categorización por medio de la conexión de ACI

El iKVM admite conexiones categorizadas con servidores y la consola de línea de comandos de CMC del iKVM, ya sea de forma local a través de un puerto de Remote Console Switch 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 ó 4161DS
- Sistema de conmutación Avocent AutoView
- Sistema de conmutación Avocent DSR
- Sistema de conmutación Avocent AMX

* No admite la conexión de consola del CMC de Dell.



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 OSCAR

En esta sección se ofrece una descripción general de la interfaz OSCAR.

Conceptos básicos de navegación

Tabla 10-1. Navegación de OSCAR con el teclado y el mouse

Tecla o secuencia de teclas	Resultado
<ul style="list-style-type: none">• <Impr Pant>-<Impr Pant>• <Mayús>-<Mayús>• <Alt>-<Alt>• <Ctrl>-<Ctrl>	Cualquiera de estas secuencias de teclas permite abrir OSCAR, en función de la configuración para Invocar OSCAR . Puede activar dos, tres o todas las secuencias de teclas si selecciona las casillas en la sección Invocar OSCAR del cuadro de diálogo Principal y hace clic en Aceptar .
<F1>	Abre la pantalla de 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 el botón 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 de edición.
<Impr Pant>, <Retroceso>	Vuelve a la selección anterior si no hubo otras pulsaciones de teclas.

Tabla 10-1. Navegación de OSCAR con el teclado y el mouse (continuación)

Tecla o secuencia de teclas	Resultado
<Impr Pant>, <Alt> + <0>	Desconecta de inmediato a un usuario de un servidor; no se selecciona ningún servidor. El indicador de estado muestra el estado Libre. (Esta acción solo se aplica a = <0> en el teclado y no en el teclado numérico.)
<Impr Pant>, <Pausa>	Enciende inmediatamente el modo de protector de pantalla e impide el acceso a esa consola específica, 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.
<Suprimir>	Elimina caracteres en un cuadro de texto.
Teclas de números	Se presionan en el teclado o en el teclado numérico.
<Bloq Mayús>	Desactivada. Para pasar de mayúsculas a minúsculas o viceversa, utilice la tecla <Mayús>.

Configuración de OSCAR

Tabla 10-2. Funciones del menú de configuración de OSCAR

Función	Propósito
Menú	Ordena la lista de servidores por número de ranura o alfabéticamente por nombre.
Security	<ul style="list-style-type: none"> • 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 de los indicadores de estado.
Idioma	Cambia el idioma de todas las pantallas de OSCAR.

Tabla 10-2. Funciones del menú de configuración de OSCAR (continuación)

Función	Propósito
Transmisión	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 hasta 16 servidores.

Para acceder al cuadro de diálogo **Configuración**:

- 1 Presione <Impr Pant> para iniciar la interfaz OSCAR. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Configuración**. Aparecerá el cuadro de diálogo **Configuración**.

Cambio de la configuración de la pantalla

Utilice el cuadro de diálogo **Menú** para cambiar el orden en que aparecen los servidores y definir un tiempo de retraso de pantalla para OSCAR.

Para acceder al cuadro de diálogo **Menú**:

- 1 Presione <Impr Pant> para abrir la interfaz OSCAR. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Configuración** y después en **Menú**. Aparece el cuadro de diálogo **Menú**.

Para elegir el orden predeterminado en que aparecen los servidores en el cuadro de diálogo **Principal**:

- 1 Seleccione **Nombre** para mostrar los servidores ordenados alfabéticamente según el nombre.
o
Seleccione **Slot** (Ranura) para visualizar los servidores ordenados por número de ranura.
- 2 Haga clic en **OK** (Aceptar).

Para asignar una o más secuencias de teclas para activar OSCAR:

Seleccione una secuencia de teclas en el menú **Invocar OSCAR** y haga clic en **Aceptar**.

La tecla predeterminada para abrir OSCAR es <Impr Pant>.

Para definir un Tiempo de retraso de pantalla para OSCAR:




- 1 Introduzca la cantidad de segundos (de 0 a 9) que tardará en abrirse la pantalla de OSCAR después de presionar <Impr Pant>. Si introduce el valor <0> OSCAR se abrirá sin retardo.
- 2 Haga clic en **OK** (Aceptar).

El tiempo de retraso de la pantalla de OSCAR permite realizar una conmutación mediante software. Para realizar una conmutación mediante software, ver “Conmutación mediante software” en la página 396.

Control 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 de cada servidor o cambiar el color, la opacidad, la imagen, la duración y la ubicación del indicador en el escritorio.

Tabla 10-3. Indicadores de estado de OSCAR

Indicador	Descripción
	Tipo de indicador por nombre
	Señala que el usuario fue desconectado de todos los sistemas
	Indica que el modo de transmisión se encuentra activado

Para acceder al cuadro de diálogo **Indicador**:



- 1 Presione <Impr Pant>. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Configuración** y después en **Indicador**. Aparecerá el cuadro de diálogo **Indicador**.

Para especificar la forma en la que aparece el indicador de estado:

- 1 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 antes de la conmutación.

 **NOTA:** Si selecciona solo la opción **Por tiempo**, el indicador no se mostrará.

- 2 Seleccione un color para el indicador en la sección **Color de imagen**. Las opciones son negro, rojo, azul y violeta.

- 3 En **Modo de visualización**, seleccione **Opaco** para que el color del indicador sea sólido o **Transparente** para ver el escritorio a través del indicador.
 - 4 Para definir la posición del indicador en el escritorio:
 - a Haga clic en **Definir posición**. Aparecerá el cuadro **Definir posición del indicador**.
 - b Haga clic con el botón izquierdo del mouse en la barra de título y arrástrela a la posición deseada en el escritorio.
 - c Haga clic con el botón derecho del mouse para regresar al cuadro de diálogo **Indicador**.
-  **NOTA:** Los cambios realizados en la posición del indicador solo se guardarán cuando haga clic en **Aceptar** en el cuadro de diálogo **Indicador**.
- 5 Haga clic 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 OSCAR para seleccionar y configurar los servidores. Además, incluye una entrada de sistema que permite establecer una conexión de consola de línea de comandos con el CMC.

Compatibilidad con periféricos

El módulo iKVM es compatible con los siguientes periféricos:

- Teclados USB estándares de PC 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 anterior del chasis Dell M1000e.



NOTA: Puede utilizar varios teclados y mouse en el puerto USB local del iKVM. El módulo 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.

Cómo ver y seleccionar servidores

Utilice el cuadro de diálogo **Principal** de OSCAR 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 RACADM o conectarse a la consola serie del servidor o a módulos de E/S.



NOTA: Los nombres y los números de ranura de los servidores los asigna el CMC.

Para acceder al cuadro de diálogo **Principal**:

Presione <Impr Pant> para iniciar la interfaz OSCAR. Aparece el cuadro de diálogo **Principal**.

o

Si se ha asignado una contraseña, aparece el cuadro de diálogo **Contraseña**. Escriba su contraseña y haga clic en **Aceptar**. Aparece el cuadro de diálogo **Principal**.

Para obtener más información sobre la configuración de una contraseña, ver “Configuración de la seguridad de la consola” en la página 398.



NOTA: Existen cuatro opciones para invocar la interfaz OSCAR. Puede activar una, varias o todas las secuencias de teclas si selecciona las casillas en la sección **Invocar OSCAR** del cuadro de diálogo **Principal** y hace clic en **Aceptar**.

Cómo ver el estado de los servidores

El estado de los servidores del chasis se indica en las columnas que se encuentran a la derecha del cuadro de diálogo **Principal**. La siguiente tabla describe los símbolos de estado.

Tabla 10-4. Símbolos de estado de la interfaz OSCAR

Símbolos	Descripción
	(Punto verde) El servidor está en línea.
	(X roja) El servidor está fuera de línea o no se encuentra en el chasis.
	(Punto amarillo) El servidor no está disponible.
	(A o B verdes) La letra indica el canal de usuario a través del cual se está accediendo al servidor: A = panel posterior, B = panel anterior.

Selección de servidores

Utilice 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 servidores:
Haga doble clic en el nombre del servidor o el número de ranura.
o
Si los servidores están ordenados por ranura (es decir, si el botón **Ranura** está presionado), escriba el número de ranura y presione <Intro>.
o
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 teclas permiten alternar entre las conexiones actual y anterior.
- Para desconectar a un usuario de un servidor:
Presione <Impr Pant> para acceder a OSCAR y haga clic en **Desconectar**.
o
Presione <Impr Pant> y después <Alt><0>. De esta forma el estado queda libre, sin servidores seleccionados. Si el indicador de estado está activo, mostrará el estado Libre en el escritorio. Vea la “Control del indicador de estado” en la página 393.

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.

Para configurar OSCAR para la conmutación mediante software:

- 1 Presione <Impr Pant> para iniciar la interfaz OSCAR. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Configuración** y después en **Menú**. Aparece el cuadro de diálogo **Menú**.
- 3 Seleccione **Nombre** o **Ranura** para la clave de orden/visualización.
- 4 Escriba el tiempo de retraso deseado expresado en segundos en el campo **Tiempo de retraso de pantalla**.
- 5 Haga clic en **OK** (Aceptar).

Para realizar una conmutación mediante software a un servidor:

- Presione <Impr Pant> para seleccionar un servidor.

Si los servidores están ordenados por ranura según la opción elegida en el paso 3 (es decir, si el botón **Ranura** está presionado), escriba el número de ranura y presione <Intro>.

o

Si los servidores están ordenados por nombre según la opción elegida en el paso 3 (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 <Retrosceso>.

Conexiones de video

El iKVM tiene conexiones de video en los paneles anterior y posterior del chasis. Las señales de conexión del panel anterior tienen prioridad respecto de las del panel posterior. Cuando un monitor se conecta al panel anterior, la conexión de video no se transmite al panel posterior y aparece un mensaje de OSCAR para indicar que las conexiones del KVM y ACI del panel posterior están desactivadas. Si el monitor se desactiva (es decir, si se quita del panel anterior o se desactiva mediante un comando del CMC), la conexión de ACI se activará y la conexión de KVM permanecerá desactivada. (Para obtener información sobre el orden de prioridad de conexión, ver “Prioridades de las conexiones del iKVM”).

Para obtener información acerca de cómo activar o desactivar la conexión del panel anterior, ver “Activación o desactivación del panel anterior”.

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 gráfica del usuario de 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 iDRAC, el usuario remoto puede desactivar la consola local en la interfaz web del iDRAC. El usuario del iKVM local recibirá un mensaje de OSCAR que indica que otro usuario se apropiará de la conexión en un plazo determinado. El usuario local deberá finalizar su trabajo antes de que se cierre la conexión del iKVM al 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, las funciones de video, teclado y mouse de ese servidor no estarán disponibles para el iKVM. El estado del servidor aparecerá marcado con un punto amarillo en el menú de OSCAR para indicar que se encuentra bloqueado o no disponible para uso local (ver “Cómo ver el estado de los servidores”).

Configuración de la seguridad de la consola

La interfaz 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.

Utilice el cuadro de diálogo **Seguridad** para bloquear la consola mediante protección por contraseña, para definir o cambiar esta contraseña o para activar el protector de pantalla.



NOTA: Si pierde u olvida la contraseña del iKVM, puede restablecer los valores predeterminados de fábrica por medio de la interfaz web del CMC o de RACADM. Ver “Eliminación de una contraseña perdida u olvidada”.

Acceso al cuadro de diálogo Seguridad

Para acceder al cuadro de diálogo Seguridad:

- 1 Presione <Impr Pant>. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Configuración** y después en **Seguridad**. Aparecerá el cuadro de diálogo **Seguridad**.

Cómo configurar o cambiar la contraseña

Para configurar o cambiar la contraseña

- 1 Haga clic una vez y presione <Intro> o haga doble clic en el campo **Nueva**.
- 2 Escriba la contraseña nueva en el campo **Nueva** y presione <Intro>. En las contraseñas se distingue entre mayúsculas y minúsculas y deben tener entre 5 y 12 caracteres. Además deben incluir al menos una letra y un número. Los caracteres válidos son: A–Z, a–z, 0–9, espacio y guión.
- 3 Escriba nuevamente la contraseña en el campo **Repetir** y presione <Intro>.
- 4 Haga clic en **Aceptar** si solo desea cambiar la contraseña y después cierre el cuadro de diálogo.

Protección por contraseña de la consola

Para proteger con contraseña la consola:

- 1 Defina la contraseña según se indica en el procedimiento anterior.
- 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 el **Modo**: si el monitor es compatible con ENERGY STAR, seleccione **Energía**; de lo contrario, seleccione **Pantalla**.



NOTA: 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 aviso emergente que indica: “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 el mouse”.



PRECAUCIÓN: Si se utiliza el modo de **Energía** en monitores no compatibles con **Energy Star**, estos pueden sufrir daños.

- 5 Opcional: para activar la prueba de protector de pantalla, haga clic en **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**.

Inicio de sesión

Para abrir la interfaz OSCAR.

- 1 Presione <Impr Pant> para abrir la interfaz OSCAR. Aparecerá el cuadro de diálogo **Contraseña**.
- 2 Escriba la contraseña y haga clic en **Aceptar**. Aparecerá el cuadro de diálogo **Principal**.

Configuración de la desconexión automática

Puede configurar la interfaz OSCAR para que se desconecte automáticamente de un servidor después de un período de inactividad.

- 1 En el cuadro de diálogo **Principal**, haga clic en **Configuración** y después en **Seguridad**.
- 2 En el campo **Tiempo de inactividad**, introduzca la cantidad de tiempo que desea permanecer conectado a un servidor antes de que se produzca la desconexión automática.
- 3 Haga clic en **OK** (Aceptar).

Eliminación de la protección por contraseña de la consola

Para eliminar la protección de la 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** si solo desea eliminar la contraseña.

Activación del modo de protector de pantalla sin contraseña



NOTA: Si la consola está protegida con contraseña, primero debe eliminar dicha función. Siga los pasos del procedimiento anterior antes de proseguir con los pasos a continuación.

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 dura 10 segundos. Al finalizar, la pantalla regresará al cuadro de diálogo **Seguridad**.



NOTA: Si se activa el modo de protector de pantalla, el usuario quedará desconectado del servidor y no se seleccionará ningún servidor. El indicador de estado señalará el estado Libre.

Cómo salir 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 desactivar el protector de pantalla:

En el cuadro de diálogo **Seguridad**, deselectione la casilla **Habilitar protector de pantalla** y haga clic en **Aceptar**.

Para activar el protector de pantalla de inmediato, presione <Impr Pant> y después <Pausa>.

Eliminación de una contraseña perdida u olvidada

Si pierde u olvida la contraseña del iKVM, puede restablecer los valores predeterminados de fábrica y después cambiar la contraseña. Puede restablecer la contraseña con la interfaz web del CMC o con RACADM.

Para restablecer una contraseña perdida u olvidada del iKVM por medio de la interfaz web del CMC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 En el submenú Chasis, seleccione **iKVM**.
- 3 Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración de iKVM**.
- 4 Haga clic en **Restaurar valores predeterminados**.

A continuación puede cambiar el valor predeterminado de la contraseña por medio de OSCAR. Ver “Cómo configurar o cambiar 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 el panel anterior y Activación de la consola del CMC de Dell, si difieren de los valores predeterminados.

Para obtener más información sobre el subcomando **racresetcfg**, consulte la sección **racresetcfg** de la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Cambio de idioma

Utilice el cuadro de diálogo **Idioma** para que el texto de la interfaz OSCAR aparezca en uno de los idiomas admitidos. El texto cambiará inmediatamente al idioma seleccionado en todas las pantallas de la interfaz.

Para cambiar el idioma de OSCAR:

- 1 Presione <Impr Pant>. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Configuración** y, después, en **Idioma**. Aparecerá el cuadro de diálogo **Idioma**.
- 3 Haga clic en el botón de radio del idioma deseado y después haga clic en **Aceptar**.

Cómo ver la información de la versión

Utilice 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>. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Comandos** y después en **Mostrar versiones**. Aparecerá el cuadro de diálogo **Versión**.

En la mitad superior del cuadro de diálogo **Versión** se enumeran las versiones del subsistema del equipo.

- 3 Haga clic en 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 especificando los que desea explorar y la cantidad de segundos que cada servidor se mostrará.

Para agregar servidores a la lista de exploración:

- 1 Presione <Impr Pant>. Aparece 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 en el chasis.
- 3 Seleccione las casillas de los servidores que desea explorar.

o

Haga doble clic en el nombre del servidor o en la ranura.

o

Presione <Alt> y el número del servidor 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 el botón **Agregar/Eliminar** y haga clic en **Aceptar**.

Para eliminar un servidor de la lista **Explorar**:

- 1 En el cuadro de diálogo **Explorar**, seleccione la casilla del servidor que desea quitar.

o

Haga doble clic en el nombre del servidor o en la ranura.

o

Haga clic en el botón **Borrar** para eliminar todos los servidores de la lista **Explorar**.

- 2 Haga clic en el botón **Agregar/Eliminar** y haga clic en **Aceptar**.

Para iniciar el modo de exploración:

- 1 Presione <Impr Pant>. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Comandos**. Aparecerá el cuadro de diálogo **Comandos**.
- 3 Seleccione la casilla **Activar exploración**.
- 4 Haga clic en **OK** (Aceptar). Aparecerá un mensaje para indicar que el mouse y el teclado fueron restablecidos.
- 5 Haga clic en para cerrar el mensaje.

Para cancelar el modo de exploración:

- 1 Si la interfaz OSCAR está abierta y se muestra el cuadro de diálogo **Principal**, seleccione un servidor de la lista.

o

Si la interfaz OSCAR *no* está abierta, mueva el mouse o presione cualquier tecla. La exploración se detendrá en el servidor actualmente seleccionado.


o

Presione <Impr Pant>. Aparecerá el cuadro de diálogo **Principal**. Seleccione un servidor de la lista.

- 2 Haga clic en el botón **Comandos**. Aparecerá el cuadro de diálogo **Comandos**.
- 3 Deseleccione la casilla **Activar exploración**.


Transmisión a servidores


Puede controlar más de un servidor del sistema a la vez para asegurarse de que todos reciban la misma señal de entrada. Puede optar por transmitir pulsaciones de teclas y movimientos de mouse por separado.

 **NOTA:** Puede transmitir a hasta 16 servidores a la vez.

Para realizar la transmisión a los servidores:

- 1 Presione <Impr Pant>. Aparece el cuadro de diálogo **Principal**.
- 2 Haga clic en **Configuración** y después en **Transmisión**. Aparecerá el cuadro de diálogo **Transmisión**.

 **NOTA:** 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 para que la interpretación de las pulsaciones sea la misma. Específicamente, los modos <Bloq Mayús> y <Bloq Num> deben ser iguales en todos los teclados. Mientras el iKVM intenta enviar pulsaciones de teclas a todos los servidores seleccionados a la vez, algunos servidores pueden inhibirse y retrasar la transmisión.

 **NOTA:** 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, el uso de movimientos del mouse para la transmisión de señales a varios servidores puede producir resultados impredecibles.

- 3 Para activar el mouse y/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 y/o <Alt><M> para seleccionar la del mouse. Repita este procedimiento con los servidores adicionales.

- 4 Haga clic en **Aceptar** para guardar la configuración y regresar al cuadro de diálogo **Configuración**. Haga clic en o presione <Esc> para regresar al cuadro de diálogo **Principal**.
- 5 Haga clic en **Comandos**. Aparecerá el cuadro de diálogo **Comandos**.
- 6 Haga clic en la casilla **Activar transmisión** para activarla. Aparecerá el cuadro de diálogo **Advertencia de transmisión**.

- 7 Haga clic en **Aceptar** para activar la transmisión.
Para cancelarla y regresar al cuadro de diálogo **Comandos**, haga clic en o presione <Esc>.
- 8 Si la transmisión está activada, escriba la información y/o ejecute los movimientos del mouse que desea transmitir desde la estación de administración. Sólo se podrá acceder a los servidores de la lista.

Para desactivar la transmisión:

En el cuadro de diálogo **Comandos**, deseccione la casilla **Activar transmisión**.

Administración del iKVM desde el CMC

Activación o desactivación del panel anterior

Para activar o desactivar el acceso al iKVM desde el panel anterior por medio 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 el <valor> es 1 (activar) o 0 (desactivar).

Para obtener más información sobre el subcomando **config**, consulte la sección correspondiente en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMCU).

Para activar o desactivar el acceso al iKVM desde el panel anterior por medio de la interfaz web:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 En el árbol del sistema, seleccione iKVM. Aparecerá la página **Estado del iKVM**.
- 3 Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración de iKVM**.
- 4 Para activar, seleccione la casilla de verificación **USB/Video de panel anterior activado**.
Para activar, seleccione la casilla de verificación **USB/Video de panel anterior activado**.
- 5 Haga clic en **Aplicar** para guardar la configuración.

Activación de la consola de CMC de Dell a través de iKVM

Para permitir que el iKVM acceda a la consola de CMC de Dell mediante RACADM, abra una consola de texto serie/Telnet/SSH en CMC, inicie sesión y escriba:

```
racadm config -g cfgKVMInfo -o  
cfgKVMAccessToCMCEnable 1
```

Para activar la consola del CMC de Dell por medio de la interfaz web:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 En el árbol del sistema, seleccione iKVM. Aparecerá la página **Estado del iKVM**.
- 3 Haga clic en la ficha **Configuración**. Aparecerá la página **Configuración de iKVM**.
- 4 Seleccione la casilla de verificación **Permitir acceso a CLI del CMC desde el iKVM**.
- 5 Haga clic en **Aplicar** para guardar la configuración.

Cómo ver el estado y las propiedades 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. El estado de la condición del iKVM asociado con el chasis puede verse en la página **Condición de las propiedades del chasis** en la sección **Gráficos del chasis**.

Para ver el estado del iKVM a través de **Gráficos del chasis**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Aparecerá la página **Estado del chasis**. La sección a la derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de la condición del iKVM. El estado de la condición del iKVM se indica mediante el color del gráfico secundario del iKVM:
 - Verde: el iKVM está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación de condiciones adversas.
 - Ámbar: el iKVM está presente, pero puede estar encendido o no, o puede estar comunicándose con el CMC o no; puede existir alguna condición adversa.
 - Gris: el iKVM está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.

- 3 Pase el cursor sobre un gráfico secundario del iKVM y se mostrará el cuadro de texto o la sugerencia de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre ese iKVM.
- 4 El gráfico secundario del iKVM tiene un hipervínculo a la página de la interfaz gráfica de usuario del CMC correspondiente para proporcionar una exploración inmediata a la página **Estado del iKVM**.

Para obtener más información acerca de iKVM, ver “Uso del módulo iKVM”.

Para ver el estado del iKVM a través de la página **Estado de iKVM**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 En el árbol del sistema, seleccione **iKVM**. Aparecerá la página **Estado del iKVM**.

Tabla 10-5. Información del estado de iKVM

Elemento	Descripción
Presencia	Muestra si el módulo iKVM está Presente o Ausente .
Estado de la alimentación	Muestra el estado de alimentación del iKVM: Encendido , Apagado o N/A (ausente).
Nombre	Muestra el nombre de producto del iKVM.
Fabricante	Muestra el fabricante del iKVM.
Número de parte	Muestra el número de parte del iKVM. El número de parte es un identificador único que el proveedor proporciona.
Versión de firmware	Muestra la versión del firmware del iKVM.
Versión del hardware	Muestra la versión de hardware del iKVM.
Panel anterior conectado	Muestra si el monitor está conectado al conector VGA del panel anterior (Sí o No). Esta información se proporciona al CMC para que este determine si el usuario local tiene acceso al panel anterior del chasis.
Panel posterior conectado	Indica si el monitor está conectado al conector VGA del panel posterior (Sí o No). Esta información se proporciona al CMC para que este determine si el usuario local tiene acceso al panel anterior del chasis.

Tabla 10-5. Información del estado de iKVM (continuación)

Elemento	Descripción
Puerto de categorización conectado	El iKVM admite la perfecta categorización con conmutadores KVM externos de Dell y Avocent que utilizan hardware incorporado. Cuando el iKVM se categoriza, se puede tener acceso a los servidores del chasis por medio de la pantalla del conmutador KVM externo desde el cual se categoriza al iKVM.
USB/video del panel anterior activado	Indica si el conector VGA del panel anterior está activado (Sí o No).
Permitir acceso al CMC desde el iKVM	Indica si la consola de comandos del CMC por medio del iKVM está activada (Sí o No).

Actualización del firmware de iKVM

Es posible actualizar el firmware del iKVM por medio de la interfaz web del CMC o RACADM.

Para actualizar el firmware del iKVM por medio de la interfaz web del CMC:

- 1** Inicie sesión en la interfaz web del CMC.
- 2** Haga clic en **Chasis** en el árbol del sistema.
- 3** Haga clic en la ficha **Actualizar**. Aparecerá la página **Componentes que se pueden actualizar**.
- 4** Haga clic en el nombre del iKVM. Aparece la página **Actualización del firmware**.
- 5** 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.




NOTA: El nombre predeterminado de la imagen del firmware de iKVM es `kvm.bin`; sin embargo, el usuario lo puede cambiar.

- 6** Haga clic en **Iniciar actualización del firmware**. Aparece un cuadro de diálogo que le solicita que confirme la acción.

7 Haga clic en **Sí** para continuar. La sección **Progreso de actualización del firmware** proporciona información del estado de la actualización del firmware. Aparecerá un indicador del estado en la página mientras se carga el archivo de imagen. El tiempo para la transferencia de archivos puede variar mucho en función de la velocidad de la conexión. Cuando comienza el proceso interno de actualización, la página se actualiza automáticamente y aparece el temporizador de actualización del firmware. Instrucciones adicionales que hay que seguir:

- No utilice el botón **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 estado de la actualización se muestra en el campo **Estado de la actualización**; este campo se actualiza automáticamente durante el proceso de transferencia de archivos. Algunos exploradores antiguos no admiten estas actualizaciones automáticas. Para actualizar de forma manual el campo **Estado de la actualización**, haga clic en **Actualizar**.

 **NOTA:** La actualización puede llevar hasta un minuto para el iKVM.

Cuando se completa la actualización, el iKVM se reinicia y el nuevo firmware se actualiza y aparece en la página **Componentes que se pueden actualizar**.

Para actualizar el firmware del iKVM mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm fwupdate -g -u -a <dirección IP del servidor FTP  
o FQDN> -d <ruta_de_archivo/nombre_de_archivo> -m kvm
```

Por ejemplo:

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

Para obtener más información sobre el subcomando **fwupdate**, consulte la sección correspondiente en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM de iDRAC6 y CMC).

Solución de problemas



NOTA: Si tiene una sesión de redirección de consola activa y hay un monitor de menor resolución conectado con el iKVM, la resolución de la consola del servidor puede restablecerse si el servidor se selecciona en la consola local. Si el servidor ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Si presiona <Ctrl><Alt><F1> en el iKVM, se cambiará de Linux a consola de texto.

Tabla 10-6. Solución de problemas del iKVM

Problema	Causa probable y solución
El mensaje “El usuario fue desactivado por el control del CMC” aparece en el monitor conectado al panel anterior.	<p>La conexión del panel anterior fue desactivada por el CMC.</p> <p>Para activar el panel anterior puede utilizar la interfaz web del CMC o RACADM.</p> <p>Para activar el panel anterior por medio de la interfaz web:</p> <ol style="list-style-type: none">1 Inicie sesión en la interfaz web del CMC.2 En el árbol del sistema, seleccione iKVM.3 Haga clic en la ficha Configuración.4 Para activar, seleccione la casilla de verificación USB/Video de panel anterior activado.5 Haga clic en Aplicar para guardar la configuración. <p>Para activar el panel anterior por medio de RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1</pre>
No funciona el acceso al panel posterior.	<p>El CMC activa la configuración del panel anterior y hay un monitor conectado actualmente al panel anterior.</p> <p>Sólo se permite una conexión a la vez. La conexión del panel anterior tiene prioridad respecto de ACI y el panel posterior. Para obtener más información sobre la prioridad de conexión, ver “Prioridades de las conexiones del iKVM”.</p>

Tabla 10-6. Solución de problemas del iKVM (continuación)

Problema	Causa probable y solución
El mensaje “El usuario fue desactivado porque otro equipo se encuentra actualmente categorizado” aparece en el monitor conectado al panel posterior.	<p>Un cable de red está conectado al conector del puerto de ACI del iKVM y a un equipo KVM secundario.</p> <p>Sólo 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 anterior, ACI y después el panel posterior.</p>
El indicador LED de color ámbar del iKVM está parpadeando.	<p>Existen tres causas posibles:</p> <p>Existe un problema en el iKVM, por lo que debe reprogramarse. Para solucionar el problema, siga las instrucciones para actualizar el firmware del iKVM (ver “Actualización del firmware de iKVM”).</p> <p>El módulo iKVM está reprogramando la interfaz de consola del CMC. En este caso, la consola de CMC no se encuentra disponible temporalmente y está representada por un punto de color amarillo en la interfaz OSCAR. Este proceso requiere de hasta 15 minutos.</p> <p>El firmware del iKVM detectó un error de hardware. Para obtener información adicional, consulte el estado del iKVM.</p> <p>Para ver el estado del iKVM por medio de la interfaz web:</p> <ol style="list-style-type: none"> 1 Inicie sesión en la interfaz web del CMC. 2 En el árbol del sistema, seleccione iKVM. <p>Para ver el estado del iKVM por medio de RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:</p> <pre>racadm getkvminfo</pre>

Tabla 10-6. Solución de problemas del iKVM (continuación)

Problema	Causa probable y solución
<p>Mi 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.</p> <p>Todos los estados muestran un punto amarillo en la interfaz OSCAR.</p>	<p>La conexión del panel anterior está activada y tiene un monitor conectado. Dado que el panel anterior tiene prioridad sobre el resto de las conexiones de iKVM, los conectores ACI y del panel posterior están desactivados.</p> <p>Para activar la conexión del puerto ACI, primero debe desactivar el acceso al panel anterior o quitar el monitor que tiene conectado. Las entradas de OSCAR del conmutador KVM externo se activarán y estarán disponibles para el acceso.</p> <p>Para desactivar el panel anterior por medio de la interfaz web:</p> <ol style="list-style-type: none">1 Inicie sesión en la interfaz web del CMC.2 En el árbol del sistema, seleccione iKVM.3 Haga clic en la ficha Configuración.4 Para eliminar, deseccione la casilla de verificación USB/Video de panel anterior activado.5 Haga clic en Aplicar para guardar la configuración. <p>Para activar el panel anterior por medio de RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0</pre>

Tabla 10-6. Solución de problemas del iKVM (continuación)

Problema	Causa probable y solución
<p>En el menú de OSCAR, la conexión del CMC de Dell muestra una X de roja y no es posible establecer conexión con el CMC.</p>	<p>Existen dos causas posibles:</p> <p>La consola del CMC de Dell fue desactivada. En este caso, para activarla puede utilizar la interfaz web del CMC o RACADM.</p> <p>Para activar la consola del CMC de Dell por medio de la interfaz web:</p> <ol style="list-style-type: none"> 1 Inicie sesión en la interfaz web del CMC. 2 En el árbol del sistema, seleccione iKVM. 3 Haga clic en la ficha Configuración. 4 Seleccione la casilla de verificación Permitir acceso a CLI del CMC desde el iKVM. 5 Haga clic en Aplicar para guardar la configuración. <p>Para activar la conexión de CMC de Dell por medio de RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre> <p>El CMC no se encuentra disponible porque se está inicializando, cediendo funciones al CMC en espera o se está reprogramando. En este caso, simplemente espere hasta que el CMC finalice el proceso de inicialización.</p>
<p>El nombre de ranura de un servidor muestra el mensaje “Inicializando” en la interfaz OSCAR y no puedo seleccionarlo.</p>	<p>El servidor se está inicializando o el iDRAC de ese servidor sufrió una falla en el proceso de inicialización.</p> <p>Primero espere 60 segundos. Si el servidor aún sigue en el proceso de inicialización, el nombre de ranura aparecerá apenas finalice el proceso y podrá seleccionar el servidor.</p> <p>Si después de 60 segundos la interfaz OSCAR aún indica que la ranura se está inicializando, quite y vuelva a insertar el servidor en el chasis. Esta acción permite que iDRAC se reinicie.</p>

Administración de la red Fabric de E/S

El chasis puede tener hasta seis módulos de E/S (IOM), que pueden ser módulos de paso o de conmutación.

Los módulos de E/S se clasifican en tres grupos: A, B y C. Cada grupo tiene dos ranuras: la ranura 1 y la ranura 2. Las ranuras se designan con letras, de izquierda a derecha, a lo largo de la parte posterior del chasis: A1 | B1 | C1 | C2 | B2 | A2. Cada servidor tiene ranuras para dos tarjetas mezzanine (MC) para conectar a los módulos de E/S. La tarjeta mezzanine y el módulo de E/S correspondiente deben tener la misma red Fabric.

Las entradas y salidas del chasis se dividen en tres rutas de acceso de datos separadas, con las letras: A, B y C. Estas rutas de acceso se describen como “REDES FABRIC” y admiten el uso de Ethernet, Fibre Channel o InfiniBand. Estas rutas de acceso de redes Fabric separadas se dividen en dos “bancos” de E/S, el banco uno y el banco dos. Cada adaptador de E/S del servidor (tarjeta mezzanine o LOM) puede tener 2 ó 4 puertos, en función de su capacidad. Estos puertos se distribuyen de manera homogénea en los bancos de módulos de E/S uno y dos para permitir la redundancia. Al implementar las redes Ethernet, iSCSI o FibreChannel, distribuya los vínculos de redundancia en los bancos uno y dos para tener la máxima disponibilidad. El módulo de E/S separado se denomina con el identificador de la red Fabric y el número del banco.

Ejemplo: “A1” denota la red Fabric “A” en el banco “1”. “C2” denota la red Fabric “C” en el banco “2”.

El chasis admite tres tipos de red Fabric o de protocolo. Los módulos de E/S y las tarjetas mezzanine de un grupo deben tener tipos de red Fabric iguales o 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 ranura de la **primera tarjeta mezzanine (MC)** en cada módulo del servidor.
- En el **Grupo C**, las ranuras de los módulos de E/S están conectadas permanentemente a la ranura de la **segunda tarjeta mezzanine (MC)** en cada módulo del servidor.



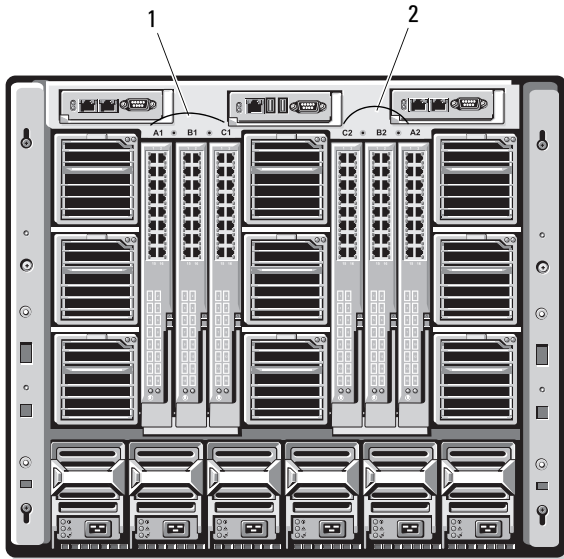
NOTA: En la CLI del CMC, los módulos de E/S se denominan con la convención switch-*n*: A1=switch-1, A2=switch-2, B1=switch-3, B2=switch-4, C1=switch-5 y C2=switch-6.

Administración de la red Fabric

La administración de la red Fabric ayuda a evitar problemas relacionados de electricidad, de configuración o de conexión debido a la instalación de un módulo de E/S o de una tarjeta mezzanine con un tipo de red Fabric no compatible con el tipo de red Fabric del chasis. Las configuraciones de hardware no válidas podrían ocasionar problemas eléctricos o funcionales en el chasis o sus componentes. La administración de la red Fabric evita que las configuraciones no válidas se activen.

La Ilustración 11-1 muestra la ubicación de los módulos de E/S en el chasis. La ubicación de cada módulo de E/S se indica por medio del número de grupo (A, B o C). Estas rutas de redes Fabric separadas se dividen en dos bancos de E/S, el banco uno y el banco dos. En el chasis, los nombres de las ranuras de los módulos de E/S están marcados como A1, A2, B1, B2, C1 o C2.

Ilustración 11-1. 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 ante configuraciones de hardware no válidas.

Por ejemplo:

- Una tarjeta mezzanine Ethernet conectada a un módulo de E/S de Fibre Channel es una configuración no válida. Sin embargo, una tarjeta mezzanine Ethernet conectada a un conmutador de Ethernet y a un módulo de E/S de paso de Ethernet instalados 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 conmutación de Fibre Channel en las ranuras B1 y B2 es una configuración válida si las primeras tarjetas mezzanine en todos los servidores también son de Fibre Channel. En este caso, el CMC activa el módulo de E/S y los servidores. Sin embargo, ciertos tipos de software de redundancia de Fibre Channel pueden no admitir esta configuración; no todas las configuraciones válidas son necesariamente configuraciones compatibles.



NOTA: La verificación de la red Fabric para los módulos de E/S y las tarjetas mezzanine del servidor solo se realiza cuando el chasis está encendido. Cuando el chasis se encuentra con alimentación en espera, los iDRAC en los módulos del servidor permanecen apagados y, por lo tanto, no pueden informar el tipo de red Fabric de las tarjetas mezzanine del servidor. Es posible que el tipo de red Fabric de las tarjetas mezzanine no se informe en la interfaz de usuario del CMC sino hasta que se encienda el iDRAC en el servidor. Además, si el chasis está encendido, la verificación de la red Fabric se realiza cuando se inserta un servidor o módulo de E/S (opcional). Si se detecta una incompatibilidad de red Fabric, se permitirá que el servidor o el módulo de E/S se enciendan y el indicador LED de estado parpadeará en color ámbar.

Configuraciones no válidas

Hay tres tipos de configuraciones no válidas:

- Configuración de tarjeta mezzanine o de LOM no válida, en la que el tipo de red Fabric del servidor recién instalado es diferente de la red Fabric del módulo de E/S ya existente
- Configuración de módulo de E/S y tarjeta mezzanine no válida, en la que el tipo de la red Fabric de un módulo de E/S recién instalado y los tipos de red Fabric de la tarjeta mezzanine residente no coinciden o no son compatibles

- Configuración de módulo de E/S y módulo de E/S no válida, en la que un módulo de E/S recién instalado tiene un tipo de red Fabric diferente o incompatible con un módulo de E/S ya instalado en el grupo

Configuración no válida de tarjeta mezzanine

Una configuración no válida de MC se produce cuando la tarjeta mezzanine o el LOM de un solo servidor no son compatibles con el módulo de E/S correspondiente. En este caso, todos los demás servidores en el chasis se pueden estar ejecutando, pero el servidor con la tarjeta MC incompatible no se podrá encender. El botón de encendido del servidor parpadeará en color ámbar para alertar acerca de una incompatibilidad de red Fabric. Para obtener información sobre los registros de CMC y de hardware, ver “Cómo ver los registros de sucesos” en la página 455.

Configuración no válida de módulo de E/S y tarjeta mezzanine

El módulo de E/S incompatible se mantendrá en estado apagado. El CMC agrega una anotación a los registros del CMC y de hardware que indica la configuración no válida y especifica el nombre del módulo de E/S. El CMC hace que el LED de error del módulo de E/S incompatible parpadee. Si el CMC está configurado para enviar alertas, enviará alertas por correo electrónico y/o alertas SNMP para este suceso. Para obtener información sobre los registros de CMC y de hardware, ver “Cómo ver los registros de sucesos” en la página 455.

Configuración no válida de módulo de E/S y módulo de E/S

El CMC mantiene el módulo de E/S recién instalado en estado apagado, hace que el LED de error del módulo de E/S parpadee y crea anotaciones en los registros del CMC y de hardware acerca de la incompatibilidad. Para obtener información sobre los registros de CMC y de hardware, ver “Cómo ver los registros de sucesos” en la página 455.

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 enciendan, 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

El estado de la condición de los módulos de E/S puede verse de dos maneras: desde la sección **Gráficos del chasis** en la página **Estado del chasis** o en la página **Estado de los módulos de E/S**. La página **Gráficos del chasis** proporciona una descripción gráfica de los módulos de E/S instalados en el chasis.

Para ver el estado de la condición de los módulos de E/S a través de Gráficos del chasis:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Aparecerá la página **Estado del chasis**. La sección derecha de **Gráficos del chasis** muestra la vista posterior del chasis y contiene el estado de la condición de los módulos de E/S. El estado de la condición del módulo de E/S se indica mediante el color del gráfico secundario del módulo de E/S:
 - Verde: el módulo de E/S está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación sobre una condición adversa.
 - Ámbar: el módulo de E/S está presente, pero es posible que esté encendido o no, o es posible que se esté comunicando con el CMC o no; puede existir alguna condición adversa.

- Gris: el módulo de E/S está presente y apagado. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.
- 3 Pase el cursor sobre un gráfico secundario individual del módulo de E/S y aparecerá un cuadro de texto o un consejo de pantalla correspondiente. El cuadro de texto proporciona información adicional sobre dicho módulo de E/S.
 - 4 El gráfico secundario del módulo de E/S tiene un hipervínculo a la página correspondiente de la interfaz gráfica de usuario del CMC para proporcionar una vía inmediata a la página **Estado del módulo de E/S** relacionada con dicho módulo de E/S.





Para ver la condición de todos los módulos de E/S a través de la página **Estado de los módulos de E/S**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Módulos de E/S** en el menú **Chasis** del árbol del sistema.
- 3 Haga clic en la ficha **Propiedades**.
- 4 Haga clic en la subficha **Estado**. Aparecerá la página **Estado de los módulos de E/S**.

Tabla 11-1. Información del estado de los módulos de E/S

Elemento	Descripción
Ranura	Muestra la ubicación del módulo de E/S en el chasis por número de grupo (A, B o C) y por banco (1 ó 2). Enumeración de módulos de E/S: A1, A2, B1, B2, C1 o C2.
Presentación	Muestra si el módulo de E/S está presente (Sí o No).

Tabla 11-1. Información del estado de los módulos de E/S (continuación)

Elemento	Descripción
Condición	 En buen estado Indica que el módulo de E/S está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar el estado de la condición del módulo de E/S.
	 Información Muestra información acerca del módulo de E/S cuando no se ha producido ningún cambio en el estado de la condición (En buen estado, Advertencia, Grave).
	 Aviso Indica que se han emitido alertas de advertencia y que se deben realizar acciones correctivas . Si no se realizan acciones correctivas, se pueden producir fallas críticas o graves que pueden afectar la integridad del módulo de E/S. Ejemplos de condiciones que causan advertencias: Incompatibilidad de la red Fabric del módulo de E/S con la red Fabric de la tarjeta mezzanine del servidor; configuración del módulo de E/S no válida, en la que los módulos de E/S recién instalados no corresponden con el módulo de E/S existente en el mismo grupo.
	 Grave Indica que se ha enviado al menos una alerta de falla. El estado Grave representa una falla del sistema en el módulo de E/S y se debe realizar una acción correctiva inmediatamente . Ejemplos de condiciones que causan un estado Grave: se detectó una falla en el módulo de E/S; se extrajo el módulo de E/S.

NOTA: Todos los cambios de la condición se anotan en los registros de hardware y del CMC. Para obtener más información, consulte "Cómo ver los registros de sucesos" en la página 455.

Tabla 11-1. Información del estado de los módulos de E/S (continuación)

Elemento	Descripción
Red Fabric	<p>Muestra el tipo de red Fabric para el módulo de E/S: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 Gbps, FC 8 Gbps, SAS 3 Gbps, SAS 6 Gbps, Infiniband SDR, Infiniband DDR, Infiniband QDR, Derivación PCIe de 1.º generación, Derivación PCIe de 2.º generación.</p> <p>NOTA: Para evitar incompatibilidades de módulos de E/S en el mismo grupo, es crucial conocer los tipos de red Fabric de los módulos de E/S en el chasis. Para obtener información sobre la red Fabric de E/S, ver “Administración de la red Fabric de E/S” en la página 415.</p>
Nombre	Muestra el nombre del producto del módulo de E/S.
Iniciar Consola de administración de módulo de E/S	<p>Si se muestra el botón para un módulo de E/S particular, al hacer clic en el botón se inicia la consola de administración para ese módulo de E/S en una nueva ventana o ficha del explorador.</p> <p>NOTA: Esta opción solo está disponible para los módulos de E/S de conmutación. No está disponible para módulos de E/S de paso o conmutadores de Infiniband no administrados.</p> <p>NOTA: No se puede tener acceso a un módulo de E/S a que está apagado, su interfaz LAN está desactivada o no se ha asignado una dirección IP válida al módulo, no se mostrará la opción Iniciar interfaz gráfica de usuario del módulo de E/S para ese módulo de E/S.</p> <p>NOTA: Se le pedirá que inicie la sesión en la interfaz de administración de módulo de E/S.</p> <p>NOTA: Puede configurar la dirección IP del módulo de E/S mediante la interfaz gráfica de usuario del CMC, según se describe en “Configuración de valores de red para un módulo de E/S individual” en la página 425.</p>
Función	<p>Al vincular los módulos de E/S juntos, el campo Función muestra la pertenencia a apilamiento de módulos de E/S. Miembro: significa que el módulo es parte de un conjunto de apilamiento. Principal: indica que el módulo es un punto de acceso primario.</p>
Estado de la alimentación	<p>Muestra el estado de la alimentación del módulo de E/S: Encendido, Apagado o N/A (ausente).</p>

Tabla 11-1. Información del estado de los módulos de E/S (continuación)

Elemento	Descripción
Etiqueta de servicio	<p>Muestra la etiqueta de servicio del módulo de E/S. La etiqueta de servicio es un identificador exclusivo que Dell asigna para fines de asistencia técnica y mantenimiento.</p> <p>Todos los cambios de la condición se anotan en los registros de hardware y del CMC. Para obtener más información, consulte “Cómo ver los registros de sucesos” en la página 455.</p> <p>NOTA: Los módulos de paso no tienen etiquetas de servicio. Solo los módulos de conmutación tienen etiquetas de servicio.</p>

Cómo ver el estado de la condición de un módulo de E/S individual

La página **Estado del módulo de E/S** (independiente de la página **Estado de los módulos de E/S**) ofrece una descripción general de un módulo de E/S individual.





Para ver el estado de la condición de un módulo de E/S individual:

- 1** Inicie sesión en la interfaz web del CMC.
- 2** Expanda **Módulos de E/S** en el árbol del sistema. Todos los módulos de E/S (de 1 a 6) aparecen en la lista **Módulos de E/S** expandida.
- 3** Haga clic en el módulo de E/S que desea ver en la lista **Módulos de E/S** en el árbol del sistema.
- 4** Haga clic en la subficha **Estado**. Aparecerá la página **Estado de los módulos de E/S**.

Tabla 11-2. Información del estado de la condición del módulo de E/S

Elemento	Descripción
Ubicación	Muestra la ubicación del módulo de E/S en el chasis mediante el número de grupo (A, B, o C) y el número de ranura (1 ó 2). Nombres de las ranuras: A1, A2, B1, B2, C1 o C2 .
Nombre	Muestra el nombre del módulo de E/S.
Presentación	Muestra si el módulo de E/S está Presente o Ausente .

Tabla 11-2. Información del estado de la condición del módulo de E/S (continuación)

Elemento	Descripción
Condición	 En buen estado Indica que el módulo de E/S está presente y se está comunicando con el CMC. En caso de una falla de comunicación entre el CMC y el servidor, el CMC no puede obtener ni mostrar el estado de la condición del módulo de E/S.
	 Información Muestra información acerca del módulo de E/S cuando no se ha producido ningún cambio en el estado de la condición (En buen estado, Advertencia, Grave). Ejemplos de condiciones que causan un estado informativo: se detectó la presencia del módulo de E/S; un usuario solicitó un ciclo de encendido del módulo de E/S.
	 Aviso Indica que se han emitido alertas de advertencia y que se deben realizar acciones correctivas . Si no se realizan acciones correctivas, se pueden producir fallas críticas o graves que pueden afectar la integridad del módulo de E/S. Ejemplos de condiciones que causan advertencias: Incompatibilidad de la red Fabric del módulo de E/S con la red Fabric de la tarjeta mezzanine del servidor; configuración del módulo de E/S no válida, en la que los módulos de E/S recién instalados no corresponden con el módulo de E/S existente en el mismo grupo.
	 Grave Indica que se ha enviado al menos una alerta de falla. El estado Grave representa una falla del sistema en el módulo de E/S y se debe realizar una acción correctiva inmediatamente . Ejemplos de condiciones que causan un estado Grave: se detectó una falla en el módulo de E/S; se extrajo el módulo de E/S.

NOTA: Todos los cambios de la condición se anotan en los registros de hardware y del CMC. Para obtener información acerca de cómo ver los registros, ver “Cómo ver el registro de hardware” en la página 455 y “Cómo ver el registro del CMC” en la página 458.

Tabla 11-2. Información del estado de la condición del módulo de E/S (continuación)


Elemento	Descripción
Estado de la alimentación	Muestra el estado de la alimentación del módulo de E/S: Encendido , Apagado o N/A (ausente).
Etiqueta de servicio	Muestra la etiqueta de servicio del módulo de E/S. La etiqueta de servicio es un identificador exclusivo que Dell asigna para fines de asistencia técnica y mantenimiento.
Red Fabric	Muestra el tipo de red Fabric para el módulo de E/S: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 Gbps, FC 8 Gbps, SAS 3 Gbps, SAS 6 Gbps, Infiniband SDR, Infiniband DDR, Infiniband QDR, Derivación PCIe de 1.º generación, Derivación PCIe de 2.º generación. NOTA: Para evitar incompatibilidades de módulos de E/S en el mismo grupo, es crucial conocer los tipos de red Fabric de los módulos de E/S en el chasis. Para obtener información sobre la red Fabric de E/S, ver “Administración de la red Fabric de E/S” en la página 415.
Dirección MAC	Muestra la dirección MAC para el módulo de E/S. La dirección MAC es una dirección exclusiva que el proveedor del hardware asigna al dispositivo como una forma de identificación. NOTA: Los módulos de paso no tienen direcciones MAC. Solo los conmutadores tienen direcciones MAC.
Función	Muestra la pertenencia de apilamiento del módulo de E/S cuando los módulos se vinculan entre sí: <ul style="list-style-type: none">• Miembro: el módulo es parte de un conjunto de apilamiento.• Principal: el módulo es un punto de acceso primario.


Configuración de valores de red para un módulo de E/S individual


La página Configuración de los módulos de E/S le permite especificar los valores de red para la interfaz que se usa para administrar el módulo de E/S. Para los conmutadores de Ethernet, lo que se configura es el puerto de administración fuera de banda (dirección IP). El puerto de administración en banda (es decir, VLAN1) no se configura por medio de esta interfaz.



NOTA: Para cambiar los valores de la página Configuración de los módulos de E/S, se deben tener privilegios de Administrador de red Fabric A para configurar los módulos de E/S del grupo A; privilegios de Administrador de red Fabric B para configurar los módulos de E/S del grupo B, o privilegios de Administrador de red Fabric C para configurar los módulos de E/S del 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 o estar en la misma red; esto provocará 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:** Solo se muestran los módulos de E/S presentes en el chasis.

 **NOTA:** No intente configurar los valores de red del módulo de E/S para módulos de paso de Ethernet y conmutadores de Infiniband.

Para configurar los valores de red para un módulo de E/S individual:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Módulos de E/S** en el árbol del sistema. Haga clic en la subficha **Configuración**. Aparecerá la página **Configuración de los valores de red de los módulos de E/S**.
- 3 Para configurar los valores de red de los módulos de E/S, escriba/seleccione valores para las siguientes propiedades y luego haga clic en **Aplicar**.

 **NOTA:** Solo se pueden configurar los módulos de E/S que están encendidos.


 **NOTA:** La dirección IP establecida en los módulos de E/S a partir del CMC no se guarda en la configuración inicial 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 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.

Tabla 11-3. Configuración de los valores de red del módulo de E/S

Elemento	Descripción
Ranura	Muestra la ubicación del módulo de E/S en el chasis mediante el número de grupo (A, B, o C) y el número de ranura (1 ó 2). Nombres de las ranuras: A1, A2, B1, B2, C1 o C2. (El valor de ranura no se puede cambiar.)
Nombre	Muestra el nombre del producto del módulo de E/S. (El nombre del módulo de E/S no se puede cambiar).
Estado de la alimentación	Muestra el estado de la alimentación del módulo de E/S. (El estado de la alimentación no se puede cambiar desde esta página.)

Tabla 11-3. Configuración de los valores de red del módulo de E/S (continuación)

Elemento	Descripción
DHCP activado	<p>Permite que el módulo de E/S del chasis solicite y obtenga automáticamente una dirección IP del servidor de protocolo de configuración dinámica de host (DHCP).</p> <p>Valor predeterminado: seleccionado (activado).</p> <p>Si esta opción está seleccionada, el módulo de E/S obtiene automáticamente la configuración de IP (dirección IP, máscara de subred y puerta de enlace) de un servidor DHCP en la red.</p> <p>NOTA: Cuando esta función está activada, los campos de propiedades Dirección IP, Puerta de enlace y Máscara de subred (que se encuentran inmediatamente después de esta opción) están desactivados y se ignorará cualquier valor introducido previamente para estas propiedades.</p> <p>Si esta opción no está seleccionada, debe introducir manualmente una dirección IP, una puerta de enlace y una máscara de subred válidas en los campos de texto correspondientes que se encuentran inmediatamente después de esta opción.</p>
Dirección IP	Especifica la dirección IP para la interfaz de red del módulo de E/S.
Máscara de subred	Especifica la máscara de subred para la interfaz de red del módulo de E/S.
Puerta de enlace	Especifica la puerta de enlace para la interfaz de red del módulo de E/S.

Solución de problemas de los valores de red del módulo de E/S

La siguiente lista contiene elementos para solucionar problemas de los valores de red del módulo de E/S:

- El CMC puede leer la configuración de la dirección IP muy rápidamente después de un cambio de configuración; mostrará 0.0.0.0 después de hacer clic en **Aplicar**. Debe hacer clic en el botón actualizar para ver si la dirección IP está configurada correctamente en el conmutador.
- Si se comete un error al configurar la IP/máscara/puerta de enlace, el conmutador no establecerá 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 el documento *Información importante del conmutador Dell PowerConnect M6220* y el *Documento técnico del agregador de puertos Dell PowerConnect de la serie 6220*.

Solución de problemas y recuperación

Descripción general

En esta sección se explica cómo realizar tareas relacionadas con la recuperación y la solución de problemas del sistema remoto a través de la interfaz web del CMC.

- Recopilación de información de configuración, estado de errores y registros de errores.
- Administración de la alimentación en un sistema remoto.
- Administración de trabajos de Lifecycle Controller en un sistema remoto.
- Cómo ver la información del chasis.
- Cómo ver los registros de sucesos.
- Uso de la consola de diagnósticos.
- Restablecer 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.
- Cómo guardar y restablecer los valores de configuración y certificados del chasis.
- Códigos y registros de errores.

Herramientas de supervisión del chasis

Recopilación de información de configuración, registros y estado del chasis

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.

Uso

```
racadm racdump
```

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

- RACADAM mediante CLI
- RACADM remoto
- RACADM mediante Telnet

El comando `RACDUMP` puede ejecutarse de manera remota desde la petición de comando de la consola serie, Telnet o SSH, o por medio de una petición de comando normal.

Para ver una lista de las opciones de sintaxis y de línea de comandos para subcomandos `RACDUMP`, escriba:

```
racadm help <racdump>
```

RACDUMP mediante CLI

Racdump incluye los siguientes subsistemas e incorpora los siguientes comandos de RACADM:

Tabla 12-1. Subsistemas y comandos RACADM

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

Uso

```
racadm racdump
```

RACDUMP remoto

RACADM remoto es una utilidad en el cliente que puede ejecutarse desde una estación de administración a través de la interfaz de red fuera de banda. Se proporciona una opción de capacidad remota **-r** que le permite conectarse al sistema administrado y ejecutar subcomandos de RACADM desde una consola remota o una estación de administración. Para utilizar la capacidad remota, necesita un nombre de usuario válido (opción **-u**) y una contraseña (opción **-p**), así como la dirección IP del 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 <nombre de archivo>`
- `racadm sslcertdownload -t <type> [-f <nombre de archivo>]`

Uso de RACDUMP remoto

Para utilizar el subcomando RACDUMP de manera remota, escriba los siguientes comandos:

```
racadm -r <dirección IP de CMC> -u <nombredeusuario>  
-p <contraseña> <subcomando> <opciones de subcomando>  
racadm -i -r <dirección IP de CMC> <subcomando>  
<opciones de subcomando>
```



NOTA: La opción `-i` indica a RACADM que solicite interactivamente el nombre de usuario y la contraseña. Sin la opción `-i`, es necesario proporcionar el nombre de usuario y la contraseña en el comando mediante las opciones `-u` y `-p`.

Por ejemplo:

```
racadm -r 192.168.0.120 -u root -p calvin racdump  
racadm -i -r 192.168.0.120 racdump
```

Si el número de puerto HTTPS del CMC se ha cambiado a un puerto personalizado diferente al predeterminado (443), se debe utilizar la siguiente sintaxis:

```
racadm -r <dirección IP CMC>:<puerto> -u  
<nombredeusuario> -p <contraseña> <subcomando>  
<opciones de subcomando>  
racadm -i -r <dirección IP de CMC>:<puerto>  
<subcomando> <opciones de subcomando>
```

RACDUMP mediante Telnet

RACDUMP mediante SSH/Telnet se utiliza para hacer referencia al uso del comando RACDUMP desde una petición de comando SSH o Telnet.

Para obtener más información sobre las instrucciones RACDUMP, consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos de iDRAC y CMC) en el sitio support.dell.com/manuals.

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, debe tener privilegios de **Administrador de configuración del chasis**.

Cómo utilizar la interfaz web

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

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Solución de problemas**.
- 4 Haga clic en la subficha **Identificar**. Aparecerá la página **Identificar**, donde se muestra una lista de todos los componentes en el chasis.
- 5 Para activar el parpadeo del LED de un componente, marque la casilla junto al nombre del dispositivo y luego haga clic en **Parpadear**.
- 6 Para desactivar el parpadeo del LED de un componente, marque la casilla junto al nombre del dispositivo y luego haga clic en **Dejar de hacer parpadear**.

Cómo utilizar de RACADM

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

```
racadm setled -m <módulo> [-1 <ledState>]
```

donde <modulo> especifica el módulo cuyo LED desea configurar. Opciones de configuración:

- `server-n` donde $n=1-16$
- `switch-n` donde $n=1-6$
- `cmc-active`

y <ledState> especifica si el LED debe parpadear. Opciones de configuración:

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

Cómo configurar alertas SNMP

Las capturas del protocolo simple de administración de red (SNMP), o *capturas de sucesos*, son similares a las alertas por correo electrónico. La estación de administración las utiliza para recibir datos no solicitados del CMC.

Se puede configurar el CMC para generar capturas de sucesos. La Tabla 12-2 proporciona una descripción general de los sucesos que desencadenan alertas de SNMP y por correo electrónico. Para obtener más información sobre las alertas por correo electrónico, ver “Configuración de alertas por correo electrónico” en la página 441.



NOTA: A partir de la versión 2.10 del CMC, SNMP es compatible con IPv6. Se puede incluir una dirección IPv6 o el nombre del dominio completamente expresado (FQDN) en el destino de un alerta de sucesos.

Tabla 12-2. Sucesos del chasis que generan alertas de SNMP y por correo electrónico

Suceso	Descripción
Falla de sonda del ventilador	Un ventilador funciona demasiado lento o no funciona.
Advertencia de sonda de baterías	Una batería ha dejado de funcionar.
Advertencia de sonda de temperatura	La temperatura está llegando a un límite excesivamente alto o bajo.
Falla de sonda de temperatura	La temperatura es demasiado alta o demasiado baja para una operación adecuada.
Redundancia degradada	La redundancia para los ventiladores y/o los suministros de energía se ha reducido.
Redundancia perdida	No hay redundancia restante para los ventiladores y/o los suministros de energía.
Aviso del suministro de energía	El suministro de energía se está acercando a una condición de falla.
Fallo del suministro de energía	El suministro de energía ha fallado.
Suministro de energía ausente	Un suministro de energía que se esperaba está ausente.
Falla de registro de hardware	El registro de hardware no funciona.
Aviso del registro de hardware	El registro de hardware está casi lleno.
Servidor ausente	Un servidor esperado no está presente.
Falla del servidor	El servidor no está funcionando.
KVM ausente	Un KVM esperado no está presente.
Fallo del KVM	El KVM no está funcionando.
Módulo de E/S ausente	Un módulo de E/S esperado no está presente.
Falla del módulo de E/S	El módulo de E/S no está funcionando.
Incompatibilidad de versión del firmware	Hay una incompatibilidad de firmware para el chasis o el firmware del servidor.

Tabla 12-2. Sucesos del chasis que generan alertas de SNMP y por correo electrónico

Suceso	Descripción
Error del umbral de alimentación del chasis	El consumo de alimentación dentro del chasis alcanzó el límite de alimentación de entrada del sistema.
Tarjeta SD ausente	No hay ningún soporte en la ranura de la tarjeta Secure Digital (SD) y una función configurada del CMC lo necesita.
Error en la tarjeta SD	Se produjo un error al acceder al soporte de la ranura de la tarjeta Secure Digital (SD) del CMC.
Error de grupo de chasis	El grupo de chasis tiene un error de configuración.

Puede agregar y configurar alertas de SNMP utilizando la interfaz web o RACADM.

Cómo utilizar la interfaz web



NOTA: Para agregar o configurar alertas de SNMP, debe tener privilegios de **Administrador de configuración del chasis**.



NOTA: Para mayor seguridad, se recomienda cambiar la contraseña predeterminada de la cuenta raíz (usuario 1). La cuenta raíz es la cuenta administrativa predeterminada que se incluye con el CMC. Para cambiar la contraseña predeterminada para la cuenta raíz, haga clic en la identificación de usuario 1 para abrir la página **Configuración de usuario**. La ayuda para esa página está disponible mediante el vínculo **Ayuda** en la esquina superior derecha de la página.

Para añadir y configurar las alertas de SNMP por medio de la interfaz web:

- 1** Inicie sesión en la interfaz web del CMC.
- 2** Seleccione **Chasis** en el árbol del sistema.
- 3** Haga clic en la ficha **Alertas**. Aparecerá la página **Sucesos del chasis**.
- 4** Active las alertas:
 - a** Seleccione las casillas de los sucesos para los que desea activar las alertas. Para activar todos los sucesos para las alertas, seleccione la casilla **Seleccionar todo**.
 - b** Haga clic en **Aplicar** para guardar la configuración.

5 Haga clic en la subficha **Configuración de capturas**. Aparecerá la página **Destino de alertas de sucesos del chasis**.

6 Escriba una dirección válida en un campo **Destino** vacío.



NOTA: Una dirección válida es una dirección que recibe las alertas de captura. Utilice el formato IPv4 “de cuatro puntos”, la notación estándar de dirección IPv6 o el FQDN. Por ejemplo: 123.123.123.123 ó 2001:db8:85a3::8a2e:370:7334 o dell.com.

7 Escriba la **Cadena de comunidad de SNMP** a la que pertenece la estación de administración de destino.



NOTA: La cadena de comunidad en la página **Destino de alertas de sucesos del chasis** es diferente de la cadena de comunidad de la página **Chasis→ Red→ Servicios**. La cadena de comunidad de capturas de SNMP es la comunidad que el CMC utiliza para capturas de salida destinadas a estaciones de administración. La cadena de comunidad en la página **Chasis→ Red→ Servicios** es la cadena de comunidad que las estaciones de administración utilizan para consultar el daemon de SNMP en el CMC.

8 Haga clic en **Aplicar** para guardar los cambios.

Para probar cuál es el destino de las alertas de una captura de sucesos:

1 Inicie sesión en la interfaz web del CMC.

2 Seleccione **Chasis** en el árbol del sistema.

3 Haga clic en la ficha **Alertas**. Aparecerá la página **Sucesos del chasis**.

4 Haga clic en la ficha **Configuración de capturas**. Aparecerá la página **Destino de alertas de sucesos del chasis**.

5 Haga clic en **Enviar** en la columna **Probar captura**, al lado del destino.



NOTA: Especifique destinos de captura como direcciones numéricas (IPv6 o IPv4) con el formato adecuado o nombres de dominio completamente expresados (FQDN). Elija un formato que sea coherente con la tecnología/infraestructura de su red. La función **Probar captura** no puede detectar elecciones incorrectas con base en la configuración de red actual (por ejemplo, el uso de un destino IPv6 en un entorno exclusivo de IPv4).

Cómo utilizar de 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. Puede ignorar el paso 2 si ya ha seleccionado una máscara de filtro.

- 2 Escriba lo siguiente para activar las alertas:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

- 3 Escriba lo siguiente para especificar los sucesos para los que desea que el CMC genere alertas:

```
racadm config -g cfgAlerting -o  
cfgAlertingFilterMask <valor de máscara>
```

donde <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 la captura de alertas para el aviso de sonda de baterías (0x2), la falla del suministro de energía (0x1000) y la falla del KVM (0x80000), ingrese 2 <O> 1000 <O> 200000 y presione la tecla <=>.

El valor hexadecimal resultante es 208002 y el valor de la máscara para el comando de RACADM es 0x208002.

Tabla 12-3. Máscaras de filtro para capturas de sucesos

Suceso	Valor de la máscara de filtro
Falla de sonda del ventilador	0x1
Advertencia de sonda de baterías	0x2
Advertencia de sonda de temperatura	0x8
Falla de sonda de temperatura	0x10
Redundancia degradada	0x40
Redundancia perdida	0x80
Aviso del suministro de energía	0x800
Fallo del suministro de energía	0x1000

Tabla 12-3. Máscaras de filtro para capturas de sucesos (continuación)

Suceso	Valor de la máscara de filtro
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
Fallo 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 de grupo de chasis	0x8000000

- 4** Escriba lo siguiente para activar las alertas de capturas:

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

donde <índice> es un valor entre 1 y 4. El CMC utiliza el número de índice para distinguir hasta cuatro destinos configurables para alertas de captura. Los destinos pueden especificarse como direcciones numéricas (IPv6 o IPv4) con el formato adecuado o nombres de dominio completamente expresados (FQDN).

- 5** Escriba lo siguiente para especificar una dirección IP de destino para recibir la alerta de capturas:

```
racadm config -g cfgTraps -o  
cfgTrapsAlertDestIPAddr <dirección IP> -i <índice>
```

donde <dirección IP> es un destino válido e <índice> es el valor del índice que se especificó en el paso 4.

6 Escriba lo siguiente para especificar el nombre de comunidad:

```
racadm config -g cfgTraps -o cfgTrapsCommunityName  
<nombre de comunidad> -i <índice>
```

donde *<nombre de comunidad>* es la comunidad SNMP a la que pertenece el chasis e *<índice>* es el valor del índice que se especificó en los pasos 4 y 5.

Se pueden configurar hasta cuatro destinos para recibir alertas de captura. 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 especifique (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba: **racadm getconfig -g cfgTraps -i <índice>**. Si el índice está configurado, aparecerán los valores para los objetos **cfgTrapsAlertDestIPAddr** y **cfgTrapsCommunityName**.

Para probar cuál es el destino de las alertas de una captura de sucesos, escriba:

```
racadm testtrap -i <índice>
```

donde *<índice>* es un valor de 1 a 4 que representa el destino de alerta que desea probar. Si no está seguro del número de índice, escriba:

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

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

En el archivo MIB SNMP del CMC se definen los tipos de chasis, los sucesos y los indicadores.

El CMC le 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:

- 1 Inicie sesión en la **interfaz web del CMC**.

- 2 Seleccione **Chasis** en el árbol del sistema.

- 3 Haga clic en **Red** → **Servicios** → **SNMP**.

Se mostrará la sección **Configuración de SNMP**.

- 4 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 la *Dell OpenManage Server Administrator SNMP Reference Guide* (Guía de referencia de SNMP de Dell OpenManage Server Administrator) en el sitio support.dell.com/manuals.

Configuración de alertas por correo electrónico

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

La Tabla 12-2 proporciona una descripción general de los sucesos que desencadenan alertas de SNMP y por correo electrónico. Para obtener más información sobre las alertas de SNMP, ver “Cómo configurar alertas SNMP” en la página 434.

Puede agregar y configurar alertas de correo electrónico a través de la interfaz web o RACADM.

Cómo utilizar la interfaz web



NOTA: Para agregar o configurar alertas de correo electrónico, debe tener privilegios de **Administrador de configuración del chasis**.

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Alertas**. Aparecerá la página **Sucesos del chasis**.
- 4 Active las alertas:
 - a Seleccione las casillas de los sucesos para los que desea activar las alertas. Para activar todos los sucesos para las alertas, seleccione la casilla **Seleccionar todo**.
 - b Haga clic en **Aplicar** para guardar la configuración.
- 5 Haga clic en la subficha **Configuración de las alertas por correo electrónico**. Aparecerá la página **Destino de alerta por correo electrónico**.
- 6 Especifique la dirección IP del servidor SMTP:
 - a Localice el campo **Servidor SMTP (correo electrónico)** y luego escriba el nombre de host SMTP o la dirección IP.



NOTA: Debe configurar el servidor de correo electrónico SMTP para aceptar correos electrónicos transmitidos desde 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.

- b** Escriba el correo electrónico originador deseado para la alerta o deje el campo en blanco para utilizar el originador de correo electrónico predeterminado. El valor predeterminado es `cmc@<dirección_IP>`, donde `<dirección_IP>` es la dirección IP del CMC. Para introducir un valor, la sintaxis del nombre del correo electrónico es `<nombre de correo electrónico>[@<dominio>]` y se puede especificar un dominio de correo electrónico de forma opcional.

Si no se especifica el valor de `@<dominio>` y hay un dominio de red del CMC activo, la dirección de correo electrónico de `<nombre de correo electrónico>@<dominio_cmc>` se utilizará como correo electrónico de origen. Si no se especifica el valor de `@<dominio>` y el CMC no tiene un dominio de red activo, se utilizará la dirección IP del CMC (por ejemplo, `<nombre de correo electrónico>@<dirección_IP>`).

- c** Haga clic en **Aplicar** para guardar los cambios.
- 7** Especifique las direcciones de correo electrónico que recibirán las alertas:
- a** Escriba una dirección de correo electrónico válida en un campo **Dirección de correo electrónico de destino** vacío.
 - b** Escriba un **Nombre** opcional. Este es el nombre de la entidad que recibirá el correo electrónico. Si se introduce un nombre para una dirección de correo electrónico no válida, este será ignorado.
 - c** Haga clic en **Aplicar** para guardar la configuración.

Para enviar un correo electrónico de prueba a un destino de alerta de correo electrónico por medio de la interfaz web del CMC:

- 1** Inicie sesión en la interfaz web del CMC.
- 2** Seleccione **Chasis** en el árbol del sistema.
- 3** Haga clic en la ficha **Alertas**. Aparecerá la página **Sucesos del chasis**.
- 4** Haga clic en la subficha **Configuración de las alertas por correo electrónico**. Aparecerá la página **Destino de alerta por correo electrónico**.
- 5** Haga clic en **Enviar** en la columna **Dirección de correo electrónico de destino** al lado del destino.

Cómo utilizar de RACADM

Para enviar un correo electrónico de prueba a un destino de alerta de correo electrónico mediante RACADM:

- 1 Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
- 2 Escriba lo siguiente para activar las 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 Escriba lo siguiente para especificar los sucesos para los que desea que el CMC genere alertas:

```
racadm config -g cfgAlerting -o  
cfgAlertingFilterMask <valor de máscara>
```

donde *<valor de máscara>* es un valor hexadecimal entre 0x0 y 0xffffffff y debe expresarse con los caracteres iniciales 0x. La Tabla 12-3 proporciona máscaras de filtro para cada tipo de suceso. Para obtener instrucciones acerca de cómo calcular el valor hexadecimal para la máscara de filtro que desea activar, consulte el paso 3 en “Cómo utilizar de RACADM” en la página 438.

- 4 Escriba lo siguiente para activar las alertas de correo electrónico:

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

donde *<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 Escriba lo siguiente para especificar la dirección de correo electrónico de destino para recibir las alertas por correo electrónico:

```
racadm config -g cfgEmailAlert -o  
cfgEmailAlertAddress <dirección de correo  
electrónico> -i <índice>
```

donde *<dirección de correo electrónico>* es una dirección de correo electrónico válida e *<índice>* es el valor del índice que se especificó en el paso 4.

- 6 Escriba lo siguiente para especificar el nombre de la persona que recibirá la alerta por correo electrónico:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEmailName <nombre de correo
electrónico> -i <índice>
```

donde *<nombre de correo electrónico>* es el nombre de la persona o grupo que recibirá la alerta por correo electrónico e *<índice>* es el valor del índice que se especificó en el paso 4 y el paso 5. El nombre de correo electrónico puede contener hasta 32 caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.

- 7 Escriba lo siguiente para configurar el host SMTP mediante la configuración de la propiedad de base de datos

```
cfgRhostsSmtServerIpAddr:
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtServerIpAddr host.domain
```

en donde *host.domain* es un nombre de dominio completamente expresado.

Puede configurar hasta cuatro direcciones de correo electrónico de destino para recibir alertas por correo electrónico. Para agregar más direcciones de correo electrónico, repita del paso 2 al paso 6.



NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice que especifique (de 1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgEmailAlert -i <índice>`. Si el índice está configurado, aparecerán los valores para los objetos `cfgEmailAlertAddress` y `cfgEmailAlertEmailName`.

Primeros pasos para solucionar problemas en un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas de alto nivel en el sistema administrado:

- 1 ¿El sistema está encendido o apagado?
- 2 Si está encendido, ¿el sistema operativo se encuentra en funcionamiento, bloqueado o simplemente inmovilizado?
- 3 Si está apagado, ¿se ha apagado de forma imprevista?

Supervisión de la alimentación y ejecución de los comandos de control de alimentación en el chasis

Puede utilizar la interfaz web o RACADM para:

- Ver el estado de alimentación actual del sistema.
- Realizar un apagado ordenado por medio del sistema operativo al reiniciar y encender o apagar el sistema.

Para obtener información acerca de la administración de la alimentación en el CMC y sobre la configuración del presupuesto de alimentación, la redundancia y el control de alimentación, ver “Administración de la alimentación” en la página 333.

Cómo ver el estado del presupuesto de alimentación

Para obtener instrucciones acerca de cómo ver el estado de presupuesto de alimentación del chasis, los servidores y las unidades de suministro de energía por medio de la interfaz web o RACADM, ver “Cómo ver el estado del consumo de alimentación” en la página 359.

Ejecución de una operación de control de alimentación

Para obtener instrucciones acerca de cómo encender, apagar, reiniciar o realizar el ciclo de encendido en el sistema por medio de la interfaz web del CMC o RACADM, ver “Ejecución de operaciones de control de alimentación en el chasis” en la página 377, “Ejecución de las operaciones de control de alimentación en un módulo de E/S” en la página 379 y “Ejecución de operaciones de control de alimentación en un servidor” en la página 380.

Solución de problemas de energía

La información siguiente le ayuda a solucionar problemas de suministro de energía y problemas relacionados con la alimentación eléctrica:

- **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.
 - **Resolución 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 soportar 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 esté disponible una configuración completa de seis unidades de suministro de energía).
 - **Resolución B:** revise si todos los suministros de energía están correctamente conectados a las dos redes de CA. Los suministros del lado 1 deben estar conectados a una red de CA, y los del lado 2 deben estar conectados a la otra red, y ambas redes de CA deben estar funcionando. La **redundancia de CA** se pierde cuando una de las dos redes no funciona.
- **Problema:** el estado de la unidad de suministro de energía se muestra como **Fallido (Sin CA)**, aun cuando hay un cable de CA conectado y la unidad está generando buena potencia de salida de CA.
 - **Resolución A:** compruebe y reemplace el cable de CA. Compruebe y confirme que la unidad de distribución de energía que proporciona la alimentación al suministro de energía funciona como se espera. Si no se soluciona el error, comuníquese con los servicios al cliente de Dell para reemplazar el suministro de energía.
 - **Resolución B:** verifique que la unidad de suministro de energía esté conectada con el mismo voltaje que las demás unidades. Si el CMC detecta que una unidad de suministro de energía funciona a diferente voltaje, la unidad se apagará y se marcará como fallida.

- **Problema:** la conexión dinámica del suministro de energía está activada, pero ninguno de los suministros de energía se muestra en el modo **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.
 - **Resolución 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 para desactivar la conexión dinámica del suministro de energía y luego volver a encenderla. Si la conexión del suministro de energía dinámica no es totalmente compatible, aparecerá un mensaje.
- **Problema:** se insertó un nuevo servidor en el gabinete con suficientes suministros de energía, pero el servidor no se enciende.
 - **Resolución A:** revise la configuración del límite de alimentación de entrada del sistema; es posible que se haya configurado demasiado bajo para permitir que se enciendan los servidores adicionales.
 - **Resolución 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.
 - **Resolución 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.
 - **Resolución D:** compruebe la prioridad de alimentación de la ranura asociada con el servidor recién insertado y asegúrese de que no esté por debajo de cualquier otra prioridad de alimentación de ranura del servidor.
- **Problema:** la alimentación disponible cambia continuamente, aun cuando no haya cambiado la configuración de gabinete modular
 - **Resolución:** la versión CMC 1.2 y versiones posteriores tienen administración dinámica de alimentación de ventiladores que reduce brevemente la asignación de alimentación a los servidores si el gabinete opera cerca de 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**. Este es el comportamiento normal.

- **Problema:** 2000 W se considera como el **Excedente para rendimiento pico**.
 - **Resolución:** 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 en esta cantidad sin afectar el rendimiento del servidor.
- **Problema:** un subconjunto de servidores perdió alimentación después de una falla de la red de CA, aun cuando el chasis estaba operando en la configuración de **Redundancia de CA** con seis suministros de energía.
 - **Resolución:** esto puede ocurrir si los suministros de energía se conectan incorrectamente a redes de CA redundantes en el momento en que ocurre la falla de la red de CA. La política de **Redundancia de CA** requiere que se conecten los tres suministros de energía de la izquierda a una red de CA, y que se conecten los tres suministros de energía de la derecha a otra red de CA. Si se conectan dos unidades de suministro de energía, por ejemplo, si PSU3 y PSU4 a las redes de CA equivocadas, un error en la red de CA ocasionará la pérdida de alimentación en los servidores de menor prioridad.
- **Problema:** los servidores de menor prioridad perdieron alimentación eléctrica después de una falla de una unidad de suministro de energía.
 - **Resolución:** este comportamiento es normal si la política de alimentación de gabinete se configuró como **Sin redundancia**. Para evitar que una falla de alimentación futuro 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 de una unidad de suministro de energía afecte la operación del servidor.
- **Problema:** el rendimiento general del servidor disminuye cuando la temperatura ambiente aumenta en el centro de datos.
 - **Resolución:** esto puede ocurrir si el **Límite de alimentación de entrada del sistema** se ha configurado con un valor que provoca una necesidad de alimentación mayor de los ventiladores que 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 que permita la asignación de alimentación adicional a los ventiladores sin afectar el rendimiento del servidor.

Administración de trabajos de Lifecycle Controller en un sistema remoto.

El servicio Lifecycle Controller está disponible en todos los servidores y lo proporciona iDRAC. CMC proporciona una lista de los trabajos de Lifecycle Controller en los servidor(es) y le permite eliminar o purgar trabajos existentes por medio de la interfaz web. Para obtener información sobre cómo activar Lifecycle Controller, ver “Actualización del firmware de los componentes de servidor mediante Lifecycle Controller” en la página 222.

La lista de trabajos de Lifecycle Controller es una lista estática de trabajos existentes en el servidor y debe actualizarse para obtener una lista más reciente y estados de los trabajos en el servidor.

Tabla 12-4 describe la información que se muestra en la lista de trabajos de Lifecycle Controller.

Tabla 12-4. Estado de los trabajos de Lifecycle Controller

Suceso	Valor de la máscara de filtro
Ranura	Muestra la ranura ocupada por el servidor en el chasis. Las ranuras son identificaciones consecutivas, de 1 a 16 (de 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.
Id. de trabajo	Número asignado por el servicio Lifecycle Controller para un trabajo en concreto.
Descripción	Frase que indica el tipo de trabajo en el servidor como trabajo de actualización, trabajo de reinicio y así sucesivamente.
Estado	Indica el estado del trabajo en el servidor.

La página de trabajos de Lifecycle Controller le permite eliminar o purgar trabajos existentes en el servidor.

Eliminación de trabajos

La operación **Eliminar** es la predeterminada y le permite eliminar todos o algunos de los trabajos en los servidores. La operación de eliminación quita los trabajos seleccionados de la cola de trabajos de Lifecycle Controller. La casilla de verificación al lado del campo **Modelo** le permite seleccionar todos los trabajos en un servidor. Se pueden seleccionar trabajos individuales mediante las casillas de verificación al lado del campo de estado del trabajo.

Purga de trabajos

La operación **Purgar** puede ser necesaria si un trabajo existente tiene un estado indeterminado y no puede eliminarse con la operación Elimiar trabajos. La operación Purgar reinicia el servicio de administración de datos, elimina todos los trabajos del servidor y puede tardar varios minutos en completarse. La casilla de verificación al lado del campo Modelo le permite seleccionar todos los trabajos para la operación Purgar.



NOTA: No se desplace a otra página después de enviar una operación para programación.

Cómo ver los resúmenes del chasis

El CMC proporciona una visión general resumida del chasis, los CMC activos y en espera, el iKVM, los ventiladores, los sensores de temperatura y los módulos de E/S.

Cómo utilizar la interfaz web

Para ver resúmenes del chasis, los CMC, el iKVM y los módulos de E/S:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Resumen**. Aparecerá la página **Resumen del chasis**.

Tabla 12-5, Tabla 12-6, Tabla 12-7, y Tabla 12-8 describa la información que aparece en la página **Resumen del chasis**.

Tabla 12-5. Resumen del chasis

Elemento	Descripción
Nombre	Muestra el nombre del chasis. El nombre identifica al chasis en la red. Para obtener información sobre la configuración del nombre del chasis, ver “Edición de los nombres de ranuras” en la página 142.
Modelo	Muestra el modelo o el fabricante del chasis. Por ejemplo, PowerEdge 2900.
Etiqueta de servicio	Muestra la etiqueta de servicio del chasis. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento.
Etiqueta de propiedad	Muestra la etiqueta de propiedad del chasis.
Ubicación	Muestra la ubicación del chasis.
Protección contra fallas del CMC lista	Muestra (Sí, No) si el CMC en espera (si está presente) es capaz de tomar el control en caso de que el CMC activo falle y ceda sus funciones.
Estado de alimentación del sistema	Muestra el estado de la alimentación del sistema.

Tabla 12-6. Resumen del CMC

Elemento	Descripción
Información del CMC activo	
Nombre	Muestra el nombre del CMC. Por ejemplo, CMC activo o CMC en espera.
Descripción	Proporciona una breve descripción del objetivo del CMC.
Fecha/Hora	Muestra la fecha y la hora definidas en el CMC activo.
Ubicación del CMC activo	Muestra la ubicación de ranura del CMC activo.
Modo de redundancia	Muestra si el CMC en espera está presente en el chasis.
Versión del firmware principal	Muestra la versión de firmware del CMC activo.

Tabla 12-6. Resumen del CMC (continuación)

Elemento	Descripción
Última actualización del firmware	Muestra la fecha en la que el firmware se actualizó por última vez. Si no se ha realizado ninguna actualización, esta propiedad mostrará el valor N/A.
Versión del hardware	Muestra la versión de hardware del CMC activo.
Dirección MAC	Muestra la dirección MAC de la interfaz de red del CMC. La dirección MAC es un identificador exclusivo del CMC en toda la red.
Dirección IP	Muestra la dirección IP de la interfaz de red del CMC.
Puerta de enlace	Muestra la puerta de enlace de la interfaz de red del CMC.
Máscara de subred	Muestra la máscara de subred de la interfaz de red del CMC.
Usa DHCP (para la dirección IP de la interfaz de red del CMC)	Muestra si el CMC está activado para solicitar y obtener una dirección IP automáticamente a partir del servidor de protocolo de configuración dinámica de host (DHCP) (Sí o No). El valor predeterminado para esta propiedad es No.
Servidor DNS principal	Muestra el nombre del servidor DNS principal.
Servidor DNS alternativo	Muestra el nombre del servidor DNS alternativo.
Utilizar DHCP para el nombre del dominio de DNS	Muestra el uso de DHCP para adquirir el nombre del dominio DNS (Sí, No).
Nombre de dominio de DNS	Muestra el nombre del dominio DNS.
Información del CMC en espera	
Presentación	Muestra (Sí, No) si hay un segundo CMC (en espera) instalado.
Versión del firmware en espera	Muestra la versión del firmware del CMC que está instalada en el CMC en espera.

Tabla 12-7. Resumen del iKVM

Elemento	Descripción
Presentación	Muestra si el módulo iKVM está presente (Sí o No).
Nombre	Muestra el nombre del iKVM. El nombre identifica al iKVM en la red.
Fabricante	Muestra el modelo o el fabricante del iKVM.
Número de parte	Muestra el número de parte del iKVM. El número de parte es un identificador único que el proveedor proporciona. Las convenciones de notación de los números de parte varían de un proveedor a otro.
Versión de firmware	Muestra la versión del firmware del iKVM.
Versión del hardware	Muestra la versión de hardware del iKVM.
Estado de la alimentación	Muestra el estado de la alimentación del iKVM: Encendido, Apagado o N/A (ausente).
USB/video del panel anterior activado	Muestra si los conectores USB y VGA del panel anterior están activados (Sí o No).
Permitir acceso a la CLI del CMC desde iKVM	Muestra si el acceso a la CLI está activado en el iKVM (Sí o No).

Tabla 12-8. Resumen del módulo de E/S

Elemento	Descripción
Ubicación	Muestra la ranura ocupada por los módulos de E/S. Las seis ranuras se identifican con un nombre de grupo (A, B o C) y un número de ranura (1 ó 2). Nombres de las ranuras: A-1, A-2, B-1, B-2, C-1 o C-2 .
Presentación	Muestra si el módulo de E/S está presente (Sí o No).
Nombre	Muestra el nombre del módulo de E/S.
Red Fabric	Muestra el tipo de red fabric.
Estado de la alimentación	Muestra el estado de la alimentación del módulo de E/S: Encendido, Apagado o N/A (ausente).
Etiqueta de servicio	Muestra la etiqueta de servicio del módulo de E/S. La etiqueta de servicio es un identificador exclusivo proporcionado por el fabricante para asistencia y mantenimiento.

Cómo utilizar de RACADM

- 1 Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
- 2 Para ver los resúmenes del chasis y del CMC, escriba:
`racadm getsysinfo`
- 3 Para ver el resumen del iKVM, escriba:
`racadm getkvminfo`
- 4 Para ver el resumen del módulo de E/S, escriba:
`racadm getioinfo`

Cómo ver el estado de la condición del chasis y de los componentes

Cómo utilizar la interfaz web

Para ver los resúmenes de la condición del chasis y de los componentes:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Seleccione **Chasis** en el árbol del sistema. Aparecerá la página **Condición del chasis**.

La sección **Gráficos del chasis** proporciona una vista gráfica frontal y posterior del chasis. La representación gráfica proporciona una descripción visual general de los componentes instalados en el chasis y su estado correspondiente.

Cada gráfico muestra una representación en tiempo real de los componentes instalados. El estado del componente se indica mediante la superposición del gráfico secundario del componente.

- Sin superposición: el componente está presente, encendido y se está comunicando con el CMC; no hay ninguna indicación de condiciones adversas.
- Señal de precaución de color ámbar: indica que solo se emitieron alertas de aviso y deben tomarse medidas correctivas.
- X de color rojo: indica que existe al menos una condición de falla. Esto significa que el CMC aún se puede comunicar con el componente y que el estado de la condición sobre la que se informa es crítico.

- Color gris: indica que el componente está presente y no está encendido. No se está comunicando con el CMC y no hay ninguna indicación de condiciones adversas.

Todos los componentes muestran un cuadro de texto o una sugerencia de pantalla correspondiente cuando el cursor se coloca sobre el gráfico secundario del componente. El estado de los componentes se actualiza en forma dinámica, y los cuadros de texto y los colores de los gráficos secundarios de los componentes se cambian automáticamente para reflejar el estado actual.

Al hacer clic en el gráfico secundario del componente se selecciona la información de ese componente y los vínculos de acceso rápido que se muestran debajo de los gráficos del chasis.

La sección Registro de hardware del CMC ofrece la últimas 10 anotaciones de ese registro como referencia.

Cómo utilizar de RACADM

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

```
racadm getmodinfo
```

Cómo ver los registros de sucesos

Las páginas **Registro de hardware** y **registro del CMC** muestran sucesos críticos del sistema que ocurren en el sistema administrado.

Cómo ver el registro de hardware

El CMC genera un registro de sucesos de hardware que ocurren en el chasis. Se puede ver el registro de hardware utilizando 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 por correo electrónico cuando ocurran sucesos específicos. Para obtener información sobre la configuración del CMC para enviar alertas, ver “Cómo configurar alertas SNMP” en la página 434 y “Configuración de alertas por correo electrónico” en la página 441.

Ejemplos de anotaciones en el registro de hardware

Suceso crítico del software del sistema:
redundancia perdida

Mié. 9 de mayo de 2007, 15:26:28 suceso normal del software del sistema: Se declaró un registro borrado

Mié. 9 de mayo de 2007, 16:06:00 suceso de aviso del software del sistema: Se declaró una predicción de falla

Mié. 9 de mayo de 2007, 15:26:31 suceso crítico del software del sistema: Se declaró un registro lleno

Mié. 9 de mayo de 2007, 15:47:23 suceso desconocido del software del sistema: Suceso desconocido

Cómo utilizar la interfaz web

Puede ver, guardar una versión en archivo de texto y borrar el registro de hardware en la interfaz web del CMC.

La Tabla 12-9 ofrece descripciones de la información proporcionada en la página **Registro de hardware** en la interfaz web del CMC.

Para ver el registro de hardware:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Registros**.
- 4 Haga clic en la subficha **Registro de hardware**. Aparecerá la página **Registro de hardware**.

Para guardar una copia del registro de hardware en la estación de administración o en la red:

- 1 Haga clic en **Guardar registro**.
Se abrirá un cuadro de diálogo.
- 2 Seleccione una ubicación para un archivo de texto del registro.








NOTA: Como el registro se guarda como archivo de texto, no aparecerán las imágenes gráficas que se utilizan para indicar la gravedad en la interfaz de usuario. En el archivo de texto, la gravedad se indica con las palabras En buen estado, Informativo, Desconocido, Advertencia y Grave. Las anotaciones de fecha y hora se guardan en orden ascendente. Si <INICIO DEL SISTEMA> aparece en la columna Fecha/Hora, significa que el suceso se presentó durante el apagado o el encendido de los módulos, cuando no se tenían fecha ni hora disponibles.

Para borrar el registro de hardware, haga clic en **Borrar registro**.



NOTA: El CMC crea una nueva anotación de registro que indica que el registro se borró.

Tabla 12-9. Información del registro de hardware

Elemento	Descripción
Gravedad	 En buen estado Indica un suceso normal que no requiere acciones correctivas.
	 Información Indica una anotación informativa en un suceso en el que el estado de Gravedad no ha cambiado.
	 Desconocido Indica un suceso no crítico que requiere que se realicen acciones correctivas con prontitud a fin de evitar fallas del sistema.
	 Aviso Indica un suceso crítico que requiere de acciones correctivas inmediatas para evitar fallas del sistema.
	 Grave Indica un suceso crítico que requiere de acciones correctivas inmediatas para evitar fallas del sistema.
Fecha/Hora	Muestra la fecha y hora exactas en la que ocurrió el suceso (por ejemplo, Mié 2 de mayo de 2007 16:26:55). Si no se muestra una fecha/hora, el suceso se produjo durante el inicio del sistema.
Descripción	Ofrece una breve descripción, generada por el CMC, del suceso (por ejemplo, Redundancy lost, Server inserted).

Cómo utilizar de RACADM

Para ver el registro de hardware mediante RACADM:

- 1 Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
- 2 Para ver el registro de hardware, escriba:

```
racadm getsel
```

Para borrar el registro de hardware, escriba:

```
racadm clrsel
```

Cómo ver el registro del CMC

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



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

Cómo utilizar la interfaz web

Se puede ver, guardar una versión en archivo de texto y borrar el registro del CMC en la interfaz web del CMC.

Podrá volver a ordenar las anotaciones de registro según el origen, fecha/hora o descripción, si hace clic en el encabezado de la columna. Si se vuelve a hacer clic en el encabezado de la columna se invertirá el orden.

La Tabla 12-10 muestra descripciones de la información proporcionada en la página **Registro del CMC** en la interfaz web del CMC.

Para ver el registro del CMC:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Registros**.
- 4 Haga clic en la subficha **Registro del CMC**. Aparecerá la página **Registro del CMC**.
- 5 Para guardar una copia del registro del CMC en la estación de administración o en la red, haga clic en **Guardar registro**.

Se abrirá un cuadro de diálogo; seleccione una ubicación para un archivo de texto del registro.

Tabla 12-10. Información del registro del CMC

Comando	Resultado
Origen	Muestra la interfaz (por ejemplo, el CMC) que provocó el suceso.
Fecha/Hora	Muestra la fecha y hora exactas en la que ocurrió el suceso (por ejemplo, Mié 2 de mayo de 2007 16:26:55).
Descripción	Ofrece una breve descripción de la acción, por ejemplo, si fue un inicio o cierre de sesión, una falla de inicio de sesión o un borrado de los registros. Las descripciones las genera el CMC.

Cómo utilizar de RACADM

Para ver la información del registro de CMC mediante RACADM:

- 1 Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
- 2 Para ver el registro de hardware, escriba:

```
racadm getraclog
```

Para borrar el registro de hardware, escriba:

```
racadm clrraclog
```

Uso de la consola de diagnósticos

La página **Consola de diagnósticos** permite a los usuarios avanzados, o a los usuarios con ayuda del personal de asistencia técnica, diagnosticar problemas relacionados con el hardware del chasis mediante comandos de la CLI.



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

Para acceder a la página de **Consola de diagnósticos**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Solución de problemas**.
- 4 Haga clic en la subficha **Diagnósticos**. Aparecerá la página **Consola de diagnósticos**.

Para ejecutar un comando CLI de diagnóstico, escriba el comando en el campo **Introducir comando de RACADM** y luego haga clic en **Enviar** para ejecutar el comando de diagnóstico. Aparecerá una página de resultados del diagnóstico.

Para regresar a la página **Consola de diagnósticos** haga clic en **Volver a la página Consola de diagnósticos** o en **Actualizar**.

La consola de diagnósticos admite los comandos que aparecen en la Tabla 12-11 así como también los comandos de RACADM.

Tabla 12-11. Comandos de diagnóstico admitidos

Comando	Resultado
arp	Muestra el contenido de la tabla del protocolo para resolución de direcciones (ARP). Las anotaciones del ARP no se pueden agregar ni eliminar.
ifconfig	Muestra el contenido de la tabla de interfaz de red.

Tabla 12-11. Comandos de diagnóstico admitidos (continuación)

Comando	Resultado
netstat	Imprime el contenido de la tabla de enrutamiento.
ping <dirección IP>	Verifica que sea posible acceder a la <dirección IP> de destino desde el CMC con el contenido actual de la tabla de enrutamiento. Debe escribir una dirección IP de destino en el campo a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de enrutamiento actual.
gettracelog	Muestra el registro de rastreo (es posible que se requieran algunos segundos para que el registro aparezca). El comando gettracelog -i muestra el número de anotaciones en el registro de rastreo. NOTA: Para obtener más información sobre el comando gettracelog , consulte la sección del comando gettracelog de la <i>RACADM Command Line Reference Guide for iDRAC7 and CMC</i> (Guía de referencia de la línea de comandos RACADM de iDRAC7 y CMC).

Restablecimiento de componentes

La página **Restablecimiento de componentes** permite que los usuarios restablezcan el CMC activo o que realicen recolocaciones virtuales de servidores que hacen que estos últimos se comporten como si se hubieran quitado e insertado nuevamente. Si el chasis tiene un CMC en espera, el restablecimiento del CMC activo hará que este último ceda sus funciones y el CMC en espera se activará.







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

Para acceder a la página de **Consola de diagnósticos**:

- 1 Inicie sesión en la interfaz web del CMC.
- 2 Haga clic en **Chasis** en el árbol del sistema.
- 3 Haga clic en la ficha **Solución de problemas**.
- 4 Haga clic en la subficha **Restablecer componentes**. Aparecerá la página **Restablecer componentes**. La sección **Resumen del CMC** de la página **Restablecer componentes** muestra la siguiente información:

Tabla 12-12. Resumen del CMC

Atributo	Descripción
Condición	<p data-bbox="329 300 471 359"> En buen estado El CMC está presente y se comunica con sus componentes.</p> <p data-bbox="329 375 999 459"> Información Muestra información acerca de CMC cuando no se ha producido ningún cambio en el estado (Normal, Advertencia, Grave).</p> <p data-bbox="329 475 999 619"> Aviso Se han emitido alertas de aviso y deben realizarse acciones correctivas. Si no se realizan acciones correctivas, existe la posibilidad de que surjan fallas críticas o graves que pueden afectar la integridad del CMC.</p> <p data-bbox="329 635 999 746"> Grave Indica que se ha emitido al menos una alerta de falla. El estado grave representa una falla del sistema CMC y se debe realizar una acción correctiva inmediatamente.</p>
Fecha/Hora	Muestra la fecha y hora para el CMC mediante el formato <i>MM/DD/AAAA</i> , en donde <i>MM</i> es el mes, <i>DD</i> es el día, y <i>AAAA</i> es el año.
Ubicación del CMC activo	Muestra la ubicación del CMC activo.
Modo de redundancia	Muestra Redundante si está presente un CMC en espera en el chasis, y Sin redundancia si no está presente un CMC en espera en el chasis.

5 La sección **Servidor de recolocación virtual** de la página **Restablecer componentes** muestra la siguiente información:

Tabla 12-13. Servidor de recolocación virtual

Atributo	Descripción
Ranura	Muestra la ranura ocupada por el servidor en el chasis. Los nombres de las ranuras son identificaciones secuenciales, de 1 a 16, que ayudan a identificar la ubicación del servidor en el chasis.
Nombre	Muestra el nombre del servidor en cada ranura.
Presentación	Indica si el servidor está presente en la ranura (Sí o No).

Tabla 12-13. Servidor de recolocación virtual (continuación)





Atributo	Descripción
Condición	<p data-bbox="292 280 434 331"> En buen estado</p> <p data-bbox="292 440 958 552"> Información Muestra información acerca del servidor cuando no se ha producido ningún cambio en el estado de la condición (En buen estado, Advertencia, Grave).</p> <p data-bbox="292 568 958 711"> Aviso Se han emitido alertas de aviso y deben realizarse acciones correctivas. Si no se toman acciones correctivas, existe la posibilidad de que surjan fallas críticas o graves que pueden afectar la integridad del servidor.</p> <p data-bbox="292 727 958 839"> Grave Indica que se ha emitido al menos una alerta de falla. El estado grave representa una falla del sistema CMC y se debe realizar una acción correctiva inmediatamente.</p>
Estado del iDRAC	<p data-bbox="292 855 958 911">Muestra el estado de la controladora incorporada de administración del iDRAC del servidor:</p> <ul data-bbox="292 927 958 1390" style="list-style-type: none"> <li data-bbox="292 927 958 951">• N/A: el servidor no está presente o el chasis no está encendido. <li data-bbox="292 967 958 991">• Listo: el iDRAC está listo y funcionando normalmente. <li data-bbox="292 1007 958 1062">• Dañado: el firmware del iDRAC está dañado. Utilice la utilidad de actualización del firmware del iDRAC para reparar el firmware. <li data-bbox="292 1078 958 1190">• Fallido: no es posible comunicarse con iDRAC. Utilice la casilla de verificación Recolocación virtual para eliminar el error. Si no funciona, desmonte manualmente el servidor y sustitúyalo para eliminar el error. <li data-bbox="292 1206 958 1294">• Actualización del firmware: actualización del firmware del iDRAC en progreso; espere a que finalice la actualización antes de intentar cualquier acción. <li data-bbox="292 1310 958 1390">• Inicializando: restablecimiento del iDRAC en progreso; espere a que se complete el encendido de la controladora antes intentar cualquier acción.

Tabla 12-13. Servidor de recolocación virtual (continuación)

Atributo	Descripción
Estado de la alimentación	Muestra el estado de la alimentación del servidor. <ul style="list-style-type: none">• N/A: el CMC no ha determinado aún el estado de la alimentación del servidor.• Apagado: el servidor, o el chasis, está apagado.• Encendido: tanto el chasis como el servidor están encendidos.• Encendiendo: estado temporal entre Apagado y Encendido. Cuando se complete el ciclo de encendido, el estado de la alimentación cambiará a Encendido.• Apagando: estado temporal entre Encendido y Apagado. Cuando se complete el ciclo de apagado, el estado de la alimentación cambiará a Apagado.
Recolocación virtual	Seleccione la casilla de verificación para recolocar el servidor de manera virtual.

- 6 Para recolocar un servidor de manera virtual, haga clic en la casilla de los servidores que desea recolocar y después seleccione **Aplicar selecciones**. Esta operación hace que los servidores se comporten como si se hubieran extraído e insertado nuevamente.
- 7 Seleccione **Restablecer/Protección contra fallas del CMC** para que se restablezca el CMC activo. Si existe un CMC en espera y el chasis es totalmente redundante, el CMC activo cede sus funciones, lo que hace que el CMC en espera se active.

Solución de problemas de errores de protocolo de hora de red (NTP)

Después de configurar el CMC para sincronizar su reloj con un servidor de tiempo remoto en la red, el cambio de hora y fecha puede llevar de 2 a 3 minutos. Si después de este tiempo no se produce el cambio, puede ser necesario solucionar algún problema. Es posible que el CMC no pueda sincronizar su reloj por diversos motivos:

- 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.

El CMC proporciona herramientas para resolver estos problemas, y el registro de rastreo del CMC constituye la fuente principal de información para la solución de problemas. Este registro contiene un mensaje de error para los errores relacionados con NTP. Si el CMC no puede sincronizarse con alguno de los servidores NTP remotos que han sido configurados, obtendrá la sincronización del reloj del sistema local.

Si el CMC está sincronizado con el reloj del sistema local y no con un servidor de tiempo remoto, el registro de rastreo tendrá una anotación similar a la siguiente:

```
8 de enero, 8 20:02:40 cmc ntpd[1423]: sincronizado
con LOCAL(0), estrato 10
```

También se puede verificar el estado de ntpd escribiendo el siguiente comando racadm:

```
racadm gettractime -n
```

Si no aparece “*” en uno de los servidores configurados, es posible que algo no esté configurado correctamente. La salida generada por el comando anterior también contiene estadísticas de NTP detalladas que pueden ser útiles para depurar los motivos por los que el servidor no se sincroniza. Si se intenta configurar un servidor NTP basado en Windows, puede ser útil aumentar el parámetro MaxDist para ntpd. Antes de cambiar este parámetro, lea y comprenda todas las consecuencias de hacerlo, especialmente porque el parámetro predeterminado debería ser lo suficientemente grande como para funcionar con la mayoría de los servidores NTP. Para modificar el parámetro, escriba el comando siguiente:

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

Luego de realizar el cambio, reinicie el ntpd de la siguiente manera: desactive el NTP, espere de 5 a 10 segundos y luego vuelva a activar el NTP.



NOTA: NTP puede requerir de 3 minutos más para intentar 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 configuran 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.

Es posible que haya otras anotaciones de registro de rastreo relacionadas con NTP que sirvan de ayuda para solucionar los problemas. Si se trata de un problema de error de configuración de la dirección IP del servidor NTP, posiblemente verá una anotación similar a:

```
8 de enero, 19:59:24 cmc ntpd[1423]: no se puede encontrar la interfaz existente para la dirección 1.2.3.4
8 de enero 8 19:59:24 cmc ntpd[1423]: la configuración de 1.2.3.4 falló
```

Si se ha configurado un valor del servidor NTP con un nombre de host no válido, posiblemente verá una anotación de registro de rastreo similar a:

```
21 de agosto 14:34:27 cmc ntpd_initres[1298]: no existe nombre de host: etc., etc., 21 de agosto 14:34:27 cmc ntpd_initres[1298]: no se pudo resolver "x", se abandona este esfuerzo
```

Para obtener información acerca de cómo se introduce el comando `gettracelog` para revisar el registro de rastreo mediante la interfaz gráfica de usuario del CMC, consulte la sección “Uso de la consola de diagnósticos” en la página 459.

Interpretación de los colores y los patrones de parpadeo de los LED

Los LED del chasis proporcionan información por medio de colores y parpadeos o la ausencia de parpadeos:

- 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 rutinario, como una carga de firmware, durante el cual la unidad no es operativa. Esto no indica una falla.
- El parpadeo de un LED de color ámbar en un módulo indica una falla en ese módulo.

- El usuario puede configurar los LED que parpadean en color azul y utilizarlos para la identificación (ver “Configuración de los LED para identificar componentes en el chasis” en la página 433).

Tabla 12-14. Colores y patrones de parpadeo de los LED

Componente	Color del LED, patrón de parpadeo	Significado
CMC	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Activo
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Luz ámbar parpadeante	Falla
	Azul, apagado	En espera
iKVM	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	Se está cargando el firmware
	Verde, apagado	Apagado
	Ámbar, encendido permanentemente	No se utiliza
	Luz ámbar parpadeante	Falla
	Ámbar, apagado	Sin fallas

Tabla 12-14. Colores y patrones de parpadeo de los LED (continuación)

Componente	Color del LED, patrón de parpadeo	Significado
Servidor	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Luz ámbar parpadeante	Falla
	Azul, apagado	Sin fallas
Módulo de E/S (común)	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal/maestro de la pila
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Luz ámbar parpadeante	Falla
	Azul, apagado	Sin fallas/esclavo de apilamiento

Tabla 12-14. Colores y patrones de parpadeo de los LED (continuación)

Componente	Color del LED, patrón de parpadeo	Significado
Módulo de E/S (de paso)	Verde, encendido permanentemente	Encendido
	Verde, parpadeando	No se utiliza
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeando	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Luz ámbar parpadeante	Falla
	Azul, apagado	Sin fallas
Ventilador	Verde, encendido permanentemente	Ventilador funcionando
	Verde, parpadeando	No se utiliza
	Verde, apagado	Apagado
	Ámbar, encendido permanentemente	Tipo de ventilador no reconocido, actualice el firmware del CMC
	Luz ámbar parpadeante	Fallo del ventilador; tacómetro fuera de rango
	Ámbar, apagado	No se utiliza
Unidad de suministro de energía	(Ovalado) Verde, encendido permanentemente	CA en buen estado
	(Ovalado) Verde, parpadeando	No se utiliza
	(Ovalado) Verde, apagado	CA en mal estado
	Ámbar, encendido permanentemente	No se utiliza
	Luz 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



NOTA: No es posible iniciar sesión en el CMC en espera por medio de una consola serie.

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, la obtención de información de recuperación a través del puerto serie DB-9 o la recuperación de la imagen del firmware del CMC.

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 alimentación. Si NO está encendido:

- 1 Verifique que haya corriente alterna presente en al menos un suministro de energía.
- 2 Verifique que la tarjeta del CMC esté asentada correctamente. Puede liberar/tirar de la palanca de expulsión, extraer el CMC y reinstalarlo asegurándose que la tarjeta esté insertada completamente y que el seguro cierre correctamente.

LED inferior: el indicador LED inferior es de varios colores. Cuando el CMC está activo y funcionando, y no hay ningún problema, el LED inferior es azul. Si es de color ámbar, se ha detectado una falla. La falla podría ser causado por cualquiera de los siguientes tres sucesos:

- Una falla del núcleo. En este caso, se debe reemplazar la tarjeta del CMC.
- Una falla de autoprueba. En este caso, se debe reemplazar la tarjeta del CMC.
- Una imagen dañada. En este caso, es posible recuperar el CMC mediante la carga de la imagen del firmware del CMC.



NOTA: Un inicio/restablecimiento normal del CMC demora un poco más de un minuto para iniciar su sistema operativo completamente y estar disponible para iniciar 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 debe estar 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 de su elección (como HyperTerminal o Minicom). Configuración: 8 bits, sin paridad, sin control de flujo, velocidad en baudios de 115200.

La falla de la memoria del núcleo hará que se muestre un mensaje de error cada 5 segundos.

- 3 Presione <Intro>. Si aparece una petición **recover**, hay información adicional disponible. La petición indicará el número de ranura del CMC y el tipo de falla.

Para mostrar el motivo de la falla y la sintaxis de algunos comandos, escriba `recover`

y luego presione <Intro>. Peticiones de ejemplo:

```
recover1 [autoprueba] falla de autoprueba del CMC 1
recover2 [imágenes de firmware dañadas] el CMC2
tiene imágenes dañadas
```

- Si la petición indica una falla de autoprueba, no hay componentes a los que se pueda dar servicio en el CMC. El CMC está dañado y debe devolverse a Dell.
- Si la petición indica **Imágenes de firmware dañadas**, siga los pasos que se indican en “Recuperación de la imagen del firmware” en la página 471 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 de actualización mediante la carga del archivo de actualización del firmware, **firming.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 al terminar.

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, usted no puede enviar comandos ping al CMC normalmente porque no hay ningún apilamiento de red activo. El comando **recover ping <IP de 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 le permite depurar los sistemas de alerta y de red del CMC. Puede acceder al registro de rastreo a través de la interfaz web del CMC (ver “Uso de la consola de diagnósticos”) o de RACADM (ver “Uso de la interfaz de línea de comandos de RACADM” y la sección de comandos **gettracelog** en la *RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC6 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 del mismo.
- 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 olvidada

 **PRECAUCIÓN: Muchas de las reparaciones solo pueden realizarlas los técnicos de servicio autorizados. 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 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 entregadas 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 patas como se muestra en la Ilustración 12-1. 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 módulo del CMC esté en un 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 Ilustración 12-1.

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 mueva la palanca hacia el lado opuesto del panel frontal del módulo. Extraiga el módulo CMC del alojamiento.



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 o acceder al CMC fuera del chasis.

- 2 Quite el conector de puente del conector de restablecimiento de contraseña e inserte un puente de dos patas para activar la cuenta predeterminada del administrador. Ver Ilustración 12-1 para localizar el puente de contraseña en la placa del CMC.

Ilustración 12-1. Ubicación del puente de restablecimiento de contraseña

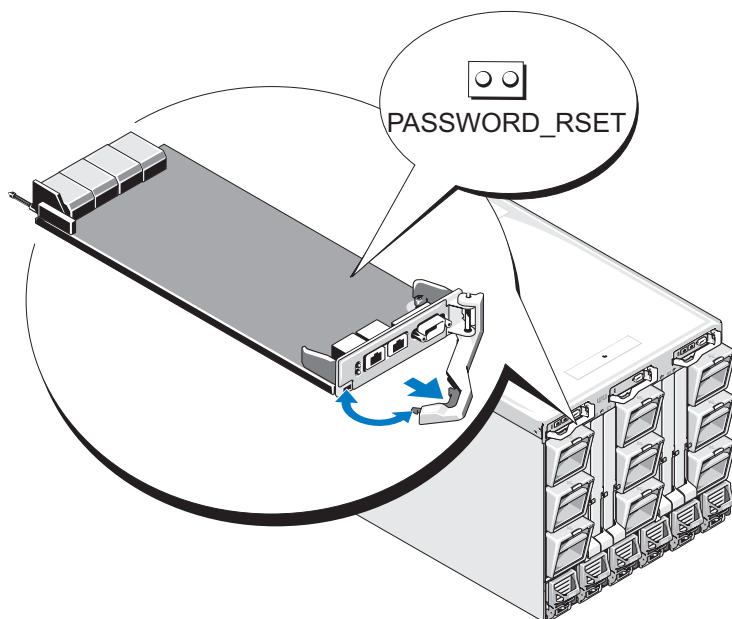




Tabla 12-15. Opciones del puente de contraseña del CMC

PASSWORD_RST		(Predet.) 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 donde se colocó el puente es el único CMC existente, simplemente espere a que termine de reiniciarse. Si cuenta con CMC redundantes en el chasis, inicie un cambio para hacer que el módulo CMC donde se colocó el puente sea el módulo activo. En la interfaz gráfica de usuario:

- a Vaya a la página **Chasis** y haga clic en la ficha **Alimentación** → subficha **Control**.
- b Seleccione el botón **Restablecer CMC (inicio activo)** 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 **raíz** y la contraseña **calvin** predeterminados de administrador, y restaure la configuración pertinente de cuenta de usuario. Las cuentas y contraseñas existentes permanecen activadas.
- 6 Realice toda acción pertinente de administración, lo que incluye la creación de una nueva contraseña de administrador que reemplace a la que se había olvidado.
- 7 Quite el puente de dos patas PASSWORD_RST y vuelva a colocar el tapón del puente.
 - a Presione el seguro de liberación del CMC en la palanca y mueva la palanca hacia el lado opuesto del panel frontal del módulo. Extraiga el módulo CMC del alojamiento.
 - b Quite el puente de dos patas 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.

Cómo guardar y restablecer los valores de configuración y certificados del chasis.

En la interfaz gráfica de usuario de CMC, vaya a **Descripción general del chasis**→ **Configuración**→ **Copia de seguridad del chasis** Aparece la pantalla **Copia de seguridad del chasis**.

Para guardar una copia de seguridad de la configuración del chasis:

- 1 En la pantalla de **Copia de seguridad del chasis**, haga clic en **Guardar**.
- 2 Suprima la ruta de acceso predeterminada para el archivo (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 para restaurar los valores y certificados de este chasis en particular.

Para restaurar la configuración del chasis:

- 1 En la pantalla de **Copia de seguridad del chasis**, haga clic en **Examinar**.
- 2 Escriba o vaya al archivo de copia de seguridad y haga clic en **Abrir** para seleccionarlo.
- 3 Haga clic en **Restaurar**.



NOTA: CMC no se reinicia al restaurar la configuración; sin embargo, los servicios del CMC pueden necesitar algo de tiempo para asimilar los cambios o la nueva configuración. Después de que se haya completado correctamente, se cerrarán todas las sesiones actuales.

Solución de problemas de alertas

Utilice el registro del CMC y el registro de rastreo para solucionar problemas de las alertas del CMC. El éxito o 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, ya 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.

Puede configurar las alertas de SNMP por medio de la interfaz web. Para obtener información, ver “Cómo configurar alertas SNMP”.

Diagnósticos

El panel LCD le permite diagnosticar problemas de cualquier servidor o módulo del chasis. Si existe un problema o un fallo en el chasis o en cualquier servidor u otro módulo del chasis, el indicador de estado del panel LCD parpadeará con una luz de color ámbar. En el Menú principal aparece un icono parpadeante con fondo de color ámbar junto a la opción correspondiente (Servidor o Gabinete) que permite acceder 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 de la opción que presenta el problema.

Para eliminar los mensajes de error del panel LCD elimine el módulo o el servidor que provoca el problema. Para eliminar los errores del servidor del LCD utilice la interfaz Web iDRAC o la interfaz de línea de comandos para borrar el registro de sucesos del sistema (SEL) del servidor.

Uso de la interfaz del panel LCD

El panel LCD puede utilizarse para tareas de configuración y diagnóstico y para obtener información de estado acerca del chasis y el contenido de este.

Navegación de la pantalla LCD

Utilice los botones situados a la derecha de la pantalla LCD para ejecutar funciones en el panel LCD. Los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia la derecha cambian los iconos u opciones de menú seleccionados en la pantalla. La opción seleccionada aparece con un fondo o borde de color azul claro.

El botón del centro activa la opción seleccionada.

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 Tabla 13-1 se utilizan para navegar entre las pantallas LCD:

Tabla 13-1. 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.
		Girar. Seleccione y presione el botón central para alternar entre las vistas gráficas de la parte anterior y posterior del chasis. NOTA: El fondo de color ámbar indica que la vista opuesta contiene errores.
		Identificación de componente. El LED de color azul parpadea en un componente. NOTA: Habrá un rectángulo azul parpadeante cerca de este icono cuando se activa la Identificación del componente .

Menú principal

Desde el menú **Principal** puede acceder 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.
- 1 Utilice los botones de flecha hacia arriba y abajo para resaltar una opción.
 - 2 Para activar la opción seleccionada, presione el botón central.

Menú de configuración del 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.
- 1 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**.
 - 2 Para activar la opción seleccionada, presione el botón central.

Pantalla de configuración de idioma

La pantalla **Configuración de idioma** permite seleccionar el idioma de los mensajes del panel LCD. El idioma activo aparece resaltado con un fondo de color azul claro.

- 1 Utilice 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 los cambios, presione el botón del centro. Aparecerá el menú **Configuración de LCD**.

Pantalla predeterminada

La opción **Pantalla predeterminada** permite cambiar la pantalla que aparece en el panel LCD cuando se encuentra inactivo. La pantalla predeterminada de fábrica es el **Menú principal**. Puede seleccionar una de las siguientes pantallas:

- **Menú principal**
- **Estado del servidor** (vista anterior del chasis)
- **Estado del módulo** (vista posterior del chasis)
- **Personalizado** (logotipo de Dell con el nombre del chasis)

La pantalla actualmente activa aparece resaltada en azul.

- 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 los cambios. 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 su estado general. La condición del servidor se indica mediante el color del icono:

- 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 del servidor indica el servidor seleccionado.

Para acceder a la pantalla **Estado gráfico del módulo**:

- 1 Seleccione el icono de giro.
- 2 Presione el botón central.

Para ver la pantalla de estado de un servidor:

- 1 Utilice los botones de flecha para resaltar el servidor deseado.
- 2 Presione el botón central. Aparecerá la pantalla **Estado del servidor**.

Para regresar al Menú principal:

- 1 Utilice los botones de flecha para resaltar el icono **Atrás**.
- 2 Presione el botón central.

Pantalla de estado gráfico del módulo

La pantalla **Estado gráfico del módulo** muestra todos los módulos instalados en la parte posterior del chasis y ofrece un resumen sobre la condición de cada módulo. La condición del módulo se indica mediante el color de cada icono, tal como se muestra a continuación:

- 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 del módulo indica el módulo seleccionado.

Para acceder a la pantalla **Estado gráfico del servidor**:

- 1 Seleccione el icono de giro.
- 2 Presione el botón central.

Para ver la pantalla de estado de un módulo:

- 1 Utilice los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia derecha para resaltar el módulo deseado.
- 2 Presione el botón central. Aparecerá la pantalla **Estado del módulo**.

Para regresar al **Menú principal**:

- 1 Utilice los botones de flecha para resaltar el icono **Atrás**.
- 2 Presione el botón central. Aparecerá el **Menú principal**.

Pantalla del menú Gabinete

Esta pantalla le permite acceder a las siguientes pantallas:

- Pantalla **Estado del módulo**
 - Pantalla **Estado del gabinete**
 - Pantalla **Resumen de IP**
 - **Menú principal**
- 1 Utilice los botones de navegación para resaltar la opción deseada (Seleccione el icono **Atrás** para regresar al **Menú principal**).
 - 2 Presione el botón central. Aparecerá la pantalla seleccionada.

Pantalla de estado del módulo

La pantalla **Estado del módulo** muestra la información y los mensajes de error de un módulo. Para ver los mensajes que pueden aparecer en esta pantalla, consulte las secciones “Información de estado del servidor y módulo de LCD” en la página 493 y “Mensajes de error de la pantalla LCD” en la página 486.

Utilice 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 un mensaje que no cabe 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 información y mensajes de error del gabinete. Ver “Mensajes de error de la pantalla LCD” en la página 486 para ver los mensajes que pueden aparecer en esta pantalla.

Utilice 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 un mensaje que no cabe la pantalla.

Seleccione el icono **Atrás** y presione el botón central para regresar a la pantalla **Estado del gabinete**.

Pantalla de resumen de IP

La pantalla **Resumen de IP** muestra información de IP del CMC y el iDRAC de cada servidor instalado.

Utilice los botones de flecha hacia arriba y abajo para desplazarse por la lista. Utilice los botones de flecha hacia la izquierda y la derecha para desplazarse por un mensaje seleccionado cuya longitud excede la pantalla.

Utilice los botones de flecha hacia arriba y abajo para seleccionar el icono **Atrás** y presione el botón central para regresar al menú **Gabinete**.

Diagnósticos

El panel LCD le permite diagnosticar problemas de cualquier servidor o módulo del chasis. Si existe un problema o un fallo en el chasis o en cualquier servidor u otro módulo del chasis, el indicador de estado del panel LCD parpadeará con una luz de color ámbar. En el **Menú principal**, un icono parpadearante con fondo de color ámbar aparece junto la opción correspondiente —Servidor o Gabinete— que permite acceder al servidor o módulo fallido.

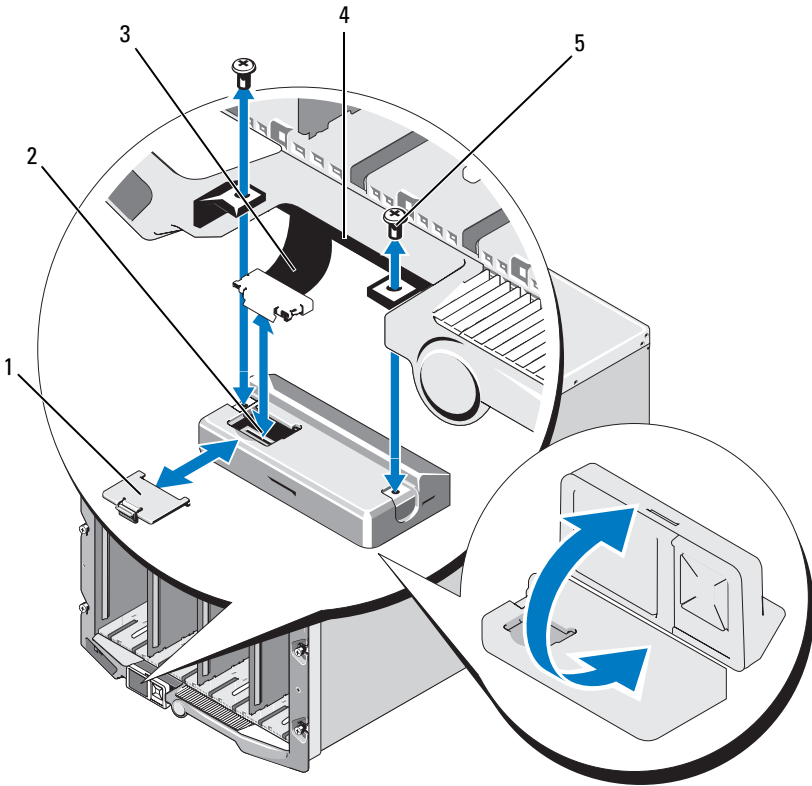
Siguiendo los iconos que parpadean en color ámbar a través del sistema de menús de la pantalla LCD, es posible visualizar la pantalla de estado y los mensajes de error de la opción que presenta el problema.

Los mensajes de error del panel LCD pueden eliminarse si se elimina el módulo o servidor que causa el problema o si se borra el registro de hardware correspondiente al módulo o al servidor. Para los errores de servidor, utilice la interfaz web de iDRAC o la interfaz de línea de comandos a fin de borrar el Registro de sucesos del sistema (SEL) del servidor. Para los errores de chasis, utilice la interfaz web del CMC o la interfaz de línea de comandos a fin de borrar el registro de hardware.

Solución de problemas del hardware LCD

Si está teniendo problemas con el LCD que estén relacionados con la utilización del CMC, utilice las siguientes opciones de solución de problemas de hardware para determinar si existe un problema con el hardware LCD o con la conexión.

Ilustración 13-1. Extracción e instalación del módulo LCD



- | | | | |
|---|--------------------|---|--------------|
| 1 | Cubierta de cables | 2 | Módulo LCD |
| 3 | Cable plano | 4 | Bisagras (2) |
| 5 | Tornillos (2) | | |

Tabla 13-2. Opciones de solución de problemas de hardware de LCD

Síntoma	Problema	Acción de recuperación
Mensaje de alerta de pantalla CMC no responde y el LED está parpadeando en color ámbar.	Pérdida de la comunicación desde el CMC al panel anterior del LCD.	Verifique que el CMC se esté iniciando; luego, reinicie el CMC a través de GUI o los comandos de RACADM.
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 fallos del CMC.	Revise el registro de hardware a través de GUI o de los comandos de RACADM. Busque un mensaje que diga: No se puede establecer la comunicación con la controladora de LCD. Recoloque 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 a través de GUI o de los comandos de RACADM. Busque un mensaje que diga: <ul style="list-style-type: none">• 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 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 anterior

Esta sección incluye dos apartados que muestran los mensajes de error y la información de estado que aparecen en la pantalla LCD del panel anterior.

Los *mensajes de error* de la pantalla LCD tienen un formato similar al del registro de sucesos del sistema (SEL) que se visualiza en la interfaz web o en CLI.

Las tablas de la sección de errores muestran los mensajes de error y aviso que aparecen en las diversas pantallas LCD y la causa posible del mensaje. El texto que aparece entre corchetes angulares (< >) indica que el texto puede variar.

La *información de estado* de la pantalla LCD incluye datos descriptivos sobre los módulos del chasis. Las tablas de esta sección describen la información que se muestra para cada componente.

Mensajes de error de la pantalla LCD

Tabla 13-3. 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 conectado.
Aviso	Se detectó una incompatibilidad de firmware o de software entre el iDRAC de la ranura <número> y el CMC.	El firmware entre los dos dispositivos no coincide para poder admitir a una o varias funciones.
Aviso	Se detectó una incompatibilidad de firmware o de software entre el BIOS del sistema de la ranura <número> y el 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 13-4. Pantalla de estado del gabinete/chasis

Gravedad	Mensaje	Causa
Crítico	Se quitó el ventilador <número>.	Este ventilador se requiere para la correcta ventilación del gabinete o el chasis.
Aviso	Se degradó la redundancia del suministro de energía.	Una o más unidades de suministro de energía fallaron o fueron eliminadas y el sistema ya no admite redundancia de unidad de suministro de energía completa.
Crítico	Se perdió la redundancia del suministro de energía.	Una o más unidades de suministro de energía fallaron o fueron eliminadas y el sistema ya no es redundante.
Crítico	Los suministros de energía no son redundantes. No hay recursos suficientes 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 hacer que los servidores se apaguen.
Aviso	La temperatura ambiente del panel de control supera el umbral máximo de aviso.	La temperatura del chasis o del gabinete supera el umbral de aviso.
Crítico	La temperatura ambiente del panel de control supera el umbral máximo de aviso.	La temperatura del chasis o del gabinete supera el umbral de aviso.
Crítico	Se perdió la redundancia de CMC.	El CMC ya no es redundante. Esto se produce al eliminar el CMC en espera.
Crítico	Todo el registro de sucesos está desactivado.	El chasis o gabinete no puede almacenar sucesos en los registros. Normalmente esto indica que hay un problema con el panel de control o el cable de panel de control.
Aviso	El registro está lleno.	El chasis ha detectado que solo se puede añadir 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 13-5. Pantallas de estado del ventilador

Gravedad	Mensaje	Causa
Crítico	La velocidad en RPM del ventilador <número> en funcionamiento está por debajo del umbral crítico mínimo.	La velocidad del ventilador indicado no es suficiente para proporcionar ventilación adecuada al sistema.
Crítico	La velocidad en RPM del ventilador <número> en funcionamiento está por encima del umbral crítico máximo.	La velocidad del ventilador no especificado es demasiado alta, lo que normalmente se debe a que una de las aspas del ventilador está rota.

Tabla 13-6. Pantallas de estado del módulo de E/S

Gravedad	Mensaje	Causa
Aviso	Se ha producido 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 un error 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 ha producido un error en el módulo de E/S <número>.	El módulo de E/S presenta un fallo. El mismo error puede presentarse si el módulo de E/S presenta problemas térmicos.

Tabla 13-7. Pantalla de estado de iKVM

Gravedad	Mensaje	Causa
Aviso	La consola no está disponible para el KVM (teclado, video y mouse) local.	Fallo menor, por ejemplo, firmware dañado.
Crítico	El KVM local no puede detectar ningún host.	Error de enumeración de host USB.
Crítico	OSCAR, que aparece en la pantalla no esta operativo para el KVM local.	Error de OSCAR.
No recuperable	El KVM local no está operativo y está apagado.	Fall de RIP serie o de chip del host USB.

Tabla 13-8. Pantallas de estado de la unidad de suministro de energía

Gravedad	Mensaje	Causa
Crítico	Se produjo un fallo en el suministro de energía <número>.	Se produjo un fallo en la unidad de suministro de energía.
Crítico	Se perdió la entrada de energía del suministro de energía <número>.	Pérdida de energía de CA o cable de CA sin conectar.
Aviso	El suministro de energía <número> 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 13-9. Pantalla de estado del servidor

Gravedad	Mensaje	Causa
Aviso	La temperatura ambiente de la placa base es inferior al umbral de aviso mínimo.	La temperatura del servidor está bajando.
Crítico	La temperatura ambiente de la placa base es inferior al umbral crítico mínimo.	La temperatura del servidor está disminuyendo.
Aviso	La temperatura ambiente del panel de control supera el umbral de aviso.	La temperatura del servidor está aumentando.
Crítico	La temperatura ambiente del panel de control supera el umbral crítico máximo.	La temperatura del servidor esta aumentando demasiado.
Crítico	La corriente del seguro de corriente de la placa base está fuera del límite permitido.	La corriente superó un umbral de fallo.
Crítico	Se produjo un fallo en la batería de la placa base.	La batería de CMOS no está presente o no tiene voltaje.
Aviso	La batería tiene un nivel de carga bajo.	La batería de la ROMB está baja.
Crítico	Se produjo un fallo en la carga de la batería.	La batería de CMOS no está presente o no tiene voltaje.

Tabla 13-9. Pantalla de estado del servidor (continuación)

Gravedad	Mensaje	Causa
Crítico	El voltaje de la CPU <número> <nombre del sensor de voltaje> ha superado el límite permitido.	
Crítico	El voltaje de la placa base del <nombre del sensor de voltaje> ha superado el límite permitido.	
Crítico	El voltaje de la tarjeta mezzanine del <número> <nombre del sensor de voltaje> ha superado el límite permitido.	
Crítico	El voltaje del almacenamiento de <nombre del sensor de voltaje> ha superado el límite permitido.	
Crítico	Se produjo un error interno (IERR) en la CPU <número>.	Fallo de la CPU.
Crítico	Se produjo un suceso 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	La CPU <número> no está presente.	La CPU requerida 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 confirmó un error de instalación.	Tarjeta mezzanine incorrecta instalada para 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 confirmó un error de instalación.	Tarjeta mezzanine incorrecta instalada para la red Fabric de E/S.

Tabla 13-9. Pantalla de estado del servidor (continuación)

Gravedad	Mensaje	Causa
Crítico	Se quitó la unidad <número de ranura>.	La unidad de almacenamiento fue eliminada.
Crítico	Se detectó un fallo en la unidad <número de ranura>.	Se produjo un fallo en la unidad de almacenamiento.
Crítico	El voltaje a prueba de errores de la placa base se encuentra fuera del 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 expiró.	El temporizador de vigilancia de iDRAC expira sin que defina una acción.
Crítico	El temporizador de vigilancia restableció el sistema.	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de reiniciar.
Crítico	El temporizador de vigilancia apagó el sistema.	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de apagado.
Crítico	El temporizador de vigilancia encendió el ciclo del sistema.	La vigilancia de iDRAC detectó que el sistema se ha bloqueado (el temporizador ha expirado porque no se ha recibido respuesta del host) y se estableció la acción de ciclo de encendido.
Crítico	El registro está lleno.	El dispositivo de 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 que se encuentra en <ubicación>.	

Tabla 13-9. Pantalla de estado del servidor (continuación)

Gravedad	Mensaje	Causa
Aviso	La tasa de errores persistentes que se pueden corregir aumentó en un dispositivo de memoria que se encuentra en <ubicación>.	Los errores de ECC que pueden corregirse alcanzaron un índice crítico.
Crítico	Se detectaron errores de varios bits en un dispositivo que se encuentra en <ubicación>.	Se detectó un error 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 genera 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 genera 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 detectó un error de paridad de PCI en un componente de la ranura <número>.	Se detectó un error de paridad en el bus PCI.
Crítico	Se detectó un error de sistema de PCI en un componente del bus <número>, dispositivo <número>, función <número>.	El dispositivo detectó un error de PCI.
Crítico	Se detectó un error de sistema de PCI en un componente de la ranura <número>.	El dispositivo detectó un error de PCI.
Crítico	De desactivó el registro de errores persistentes que se pueden corregir en un dispositivo de memoria que se encuentra en <ubicación>.	Los errores de un solo bit (SBE) se desactivan cuando se registran demasiados en un dispositivo de memoria.
Crítico	Todo el registro de sucesos está desactivado.	
No recuperable	Se detectó un error de protocolo de CPU.	El protocolo del procesador entró en un estado no recuperable.

Tabla 13-9. Pantalla de estado del servidor (continuación)

Gravedad	Mensaje	Causa
No recuperable	Se detectó un error de paridad de bus de CPU.	El PERR de bus del procesador ingresó a un estado no recuperable.
No recuperable	Se detectó un error de inicialización de CPU.	La inicialización del procesador entró en un estado no recuperable.
No recuperable	Se detectó una comprobación del equipo de CPU.	La revisión de máquina del procesador entró en un estado no recuperable.
Crítico	Se perdió la redundancia de memoria.	
Crítico	Se detectó un error fatal de bus en un componente del bus <ubicación>, dispositivo <ubicación>, función <ubicación>.	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 <número>, dispositivo <número>, función <número>.	No se pudo programar la dirección flexible para este dispositivo.
Crítico	La opción ROM del dispositivo de una tarjeta mezzanine <número> no pudo admitir el ajuste de vínculos o FlexAddress.	La ROM de opción no admite la dirección flexible 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 la “Guía de usuario del servidor”.

Información de estado del servidor y módulo de LCD

Las tablas que figuran en esta sección describen las opciones de estado que se muestran en la pantalla LCD del panel anterior para cada tipo de componente del chasis.

Tabla 13-10. Estado del CMC

Elemento	Descripción
Ejemplo: CMC1, CMC2	Nombre/Ubicación
Sin errores	Si no se produce ningún error, aparecerá el mensaje “Sin errores”, en caso contrario se mostrará la lista de errores.
Versión de firmware	Solo se muestra en un CMC activo. Muestra En espera para el CMC en espera.
IP4 <activado, desactivado>	Muestra el estado actual activado de IPv4 únicamente en un CMC activo.
Dirección IP4: <address, acquiring>	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 13-11. Estado del chasis/gabinete

Elemento	Descripción
Nombre definido por el usuario	Ejemplo: “Sistema de bastidor Dell”. Esta opción puede configurarse a través de la CLI o la interfaz gráfica del usuario web del CMC.
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.
Número de modelo	Ejemplo: “PowerEdgeM1000”.
Consumo de energía	Consumo de energía actual en vatios.
Máxima energía	Consumo máximo de energía en vatios.
Mínima energía	Consumo mínimo de energía en vatios.
Temperatura ambiente	Temperatura ambiente actual en grados Celsius.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.

Tabla 13-11. Estado del chasis/gabinete (continuación)

Elemento	Descripción
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 de CC.

Tabla 13-12. Estado del ventilador

Elemento	Descripción
Nombre/Ubicación	Ejemplo: Ventilador1, Ventilador2, etc.
Mensajes de error	Si no existen errores se muestra el mensaje “Sin errores”. De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y, a continuación, los avisos.
RPM	Velocidad actual del ventilador en RPM

Tabla 13-13. Estado de la unidad de suministro de energía

Elemento	Descripción
Nombre/Ubicación	Ejemplo: PSU1, PSU2, etc.
Mensajes de error	Si no existen errores se muestra el mensaje “Sin errores”. De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y, a continuación, los avisos.
Estado	Desconectado, conectado o en espera
Potencia máxima	Potencia máxima que la unidad de suministro de energía puede proporciona al sistema

Tabla 13-14. Estado del módulo de E/S

Elemento	Descripción
Nombre/Ubicación	Ejemplo: IOM A1, IOM B1. etc.

Tabla 13-14. Estado del módulo de E/S

Elemento	Descripción
Mensajes de error	Si no existen errores se muestra el mensaje “Sin errores”. De lo contrario, aparecen los mensajes de error, con los errores críticos en primer lugar y, a continuación, los avisos.
Estado	Encendido o apagado
Modelo	Modelo del módulo de E/S
Tipo de estructura de red	Tipo de sistema de red
Dirección IP	Sólo aparece si el módulo de E/S está encendido. Este valor es cero para un módulo de E/S de conmutación.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.

Tabla 13-15. Estado del iKVM

Elemento	Descripción
Nombre	iKVM.
Sin errores	Si no hay errores, se mostrará el mensaje Sin errores , en caso contrario aparecerá la lista de los mensajes de error. Primero aparecen lo errores críticos, seguidos de los avisos. Para obtener más información, ver “Mensajes de error de la pantalla LCD”.
Estado	Encendido o apagado.
Modelo/fabricante	Descripción del modelo de iKVM.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.
Número de parte	Número de pieza del fabricante.
Versión de firmware	Versión del firmware de iKVM.
Versión del hardware	Versión de hardware de iKVM.

NOTA: Esta información se actualiza de forma dinámica.

Tabla 13-16. Estado del servidor

Elemento	Descripción
Ejemplo: Servidor 1, Servidor 2, etc.	Nombre/Ubicación

Tabla 13-16. Estado del servidor (continuación)

Elemento	Descripción
Sin errores	Si no hay errores, se mostrará el mensaje Sin errores , en caso contrario aparecerá la lista de los mensajes de error. Primero aparecen los errores críticos, seguidos de los avisos. Para obtener más información, ver “Mensajes de error de la pantalla LCD”.
Nombre de ranura	Nombre de ranura de chasis. Por ejemplo, RANURA-01. NOTA: Puede establecer esta tabla mediante la CLI o la interfaz gráfica del usuario web del CMC.
Nombre	Nombre del servidor, que el usuario puede establecer mediante Dell OpenManage. El nombre se muestra solamente si iDRAC se inició completamente y el servidor admite esta función. En caso contrario se mostrarán los mensajes de inicio de iDRAC.
Número de modelo	Muestra si el iDRAC completó el inicio.
Etiqueta de servicio	Muestra si el iDRAC completó el inicio.
Versión del BIOS	Versión del firmware del BIOS del servidor.
Código de última publicación	Muestra la cadena de mensajes del código de la última publicación del BIOS del servidor.
Versión del firmware del iDRAC	Muestra si el iDRAC completó el inicio. NOTA: La versión 1.01 de iDRAC se muestra como 1.1. No existe la versión 1.10 de iDRAC.
IP4 <activado, desactivado>	Muestra el estado actual activado del IPv4.
Dirección IP4: <address, acquiring>	Solo se muestra si IPv4 está activado.
IP6 <activado, desactivado>	Solo se muestra si iDRAC admite IPv6. Muestra el estado actual activado del IPv6.
Dirección local IP6: <dirección>	Solo muestra si iDRAC admite IPv6 y si IPv6 está activado.
Dirección global IP6: <dirección>	Solo muestra si iDRAC admite IPv6 y si IPv6 está activado.

Tabla 13-16. Estado del servidor (continuación)

Elemento	Descripción
FlexAddress activado en la red Fabric	Solo se muestra si la función está instalada. Muestra una lista de las redes fabric activadas para este servidor (es decir, A, B, C).

La información de Tabla 13-16 se actualiza de forma dinámica. Si el servidor no admite esta función, no aparecerá la información siguiente, además, las opciones del Server Administrator son las siguientes:

- Opción “Ninguna” = No se debe mostrar ninguna cadena en el LCD.
- Opción “Predeterminada” = Ningún efecto.
- Opción “Personalizada” = Le permite introducir un nombre de cadena para el servidor.

Solo se muestra la información si iDRAC se ha iniciado completamente. Para obtener más información sobre esta función, consulte la *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC7 y CMC).

Índice

A

- ACI, 389
- Activación de FlexAddress Plus, 279
- Activación o desactivación de DCHP, 91
- Active Directory, 281
 - cómo agregar usuarios del CMC, 302
 - cómo extender esquemas, 295
 - cómo usarlo con el esquema estándar, 282
 - configuración de acceso al CMC, 294
 - configuración y administración de certificados, 182
 - extensiones de esquema, 289
 - objetos, 290
- administración de redes
 - Fabric, 415
- agregar
 - alertas de SNMP, 434
- alertas
 - solución de problemas, 476
- Alertas de SNMP
 - cómo agregar y configurar, 434
- archivo de configuración
 - creación, 105

C

- capa de sockets seguros (SSL)
 - acerca de, 193
- certificado de servidor
 - cómo cargar, 199
 - cómo ver, 201
- certificados
 - Active Directory, 182
 - carga de un certificado de servidor, 199
 - cómo ver un certificado de servidor, 201
 - SSL y digitales, 193
- CMC
 - configuración, 35, 305
 - conjuntos de funciones, 23
 - creación de un archivo de configuración, 105
 - descarga del firmware, 56
 - entorno redundante, 60
 - instalación, 35
 - registro, 458
- Cómo ver la configuración de la red actual de IPv4, 88
- Cómo ver la configuración de la red actual de IPv6, 88
- complemento
 - instalación de la extensión de Dell, 301

- conectar comando
 - conexión de la línea de comandos del CMC, 71
- conexión de acceso remoto (RAC), 28
- configuración
 - CMC desde el panel LCD, 56
 - presupuesto de alimentación, 56
 - RACADM remoto, 55
 - RACADM remoto del CMC, 55
- Configuración de la red LAN, 89
- configuración del CMC, 35
- Configuración y administración de los servicios genéricos de protocolo ligero de acceso a directorios, 189
- configurar
 - alertas de SNMP, 434
- conjuntos de funciones del CMC, 23
- conservación de alimentación, 346
- consola de línea de comandos
 - funciones, 65
- consola serie
 - uso, 66
- consola Telnet
 - uso, 66
- contraseña
 - deshabilitar, 472
 - restablecer la colocación del puente, 474

E

- entorno redundante, 60
- especificaciones
 - hardware, 27
- especificaciones de hardware, 27
- esquema estándar
 - cómo usarlo con Active Directory, 282
- estación de administración
 - configuración de la emulación de terminal, 69
- explorador de web
 - exploradores admitidos, 29
- explorador web
 - configuración, 43

F

- firmware
 - actualización, CMC, 214
 - actualización, dispositivo de infraestructura del módulo de E/S, 218
 - actualización, iKVM, 216
 - actualización, servidor iDRAC, 219
 - administración, 212
 - cómo descargar, 56

FlexAddress, 257
 activación, 258
 cómo ver el estado a través de la CLI, 265
 configuración a través de la CLI, 263
 configuración de Linux, 264
 contrato de licencia, 273
 desactivación, 262
 encendido en LAN, 266
 solución de problemas, 266
 verificación de activación, 260

I

iDRAC
 recuperación de firmware, 220
iKVM, 387
Inicio de sesión único, 314
Instalación del CMC, 35
Interfaz de consola
 analógica, 387
interfaz web
 acceso, 115
 configuración de alertas por correo electrónico, 441

M

Microsoft Active Directory, 281

N

nombres de ranuras
 cómo asignar nombres a reglas, 142
 edición, 142

O

OSCAR, 387

P

panel LCD
 configuración de la CMC a partir de, 56
Preguntas frecuentes
 uso del CMC con Active Directory, 311
preguntas frecuentes
 administración y recuperación de un sistema remoto, 253, 277
presupuesto de alimentación
 configuración, 56
propiedades de red
 configuración manual, 88
 configuración por medio de racadm, 88

R

RAC
 consulte Conexión de acceso remoto, 28

RACADM

- desinstalación de la estación de administración de Linux, 42

RACADM remoto

- configuración, 55

Red Fabric de E/S, 415

Red Hat Enterprise Linux

- configuración para redirección de consola serie, 74

registro de hardware, 455

registros

- CMC, 458

- hardware, 455

reglas del análisis, 107

S

seguridad

- cómo usar los certificados SSL y digitales, 193

servicios

- configuración, 202

servidor proxy, 43

sistema administrado

- acceso por medio del puerto serie local, 66

solicitud de firma de certificado (CSR)

- acerca de, 194

- cómo generar un nuevo certificado, 195

T

- tarjeta de función, 260

U

- Uso de FlexAddress Plus, 280

utilidad racadm

- configuración de las propiedades de red, 88

- reglas de análisis, 107

V

- VLAN de CMC, 94

W

- WS-Management, 29