Chassis Management Controller versión 2.0 para Dell PowerEdge VRTX

Guía del usuario



Notas, precauciones y avisos

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

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

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

Copyright © 2014 Dell Inc. Todos los derechos reservados. Este producto está protegido por leyes internacionales y de los Estados Unidos sobre los derechos de autor y la protección intelectual. Dell™ y el logotipo de Dell son marcas comerciales de Dell Inc. en los Estados Unidos y en otras jurisdicciones. El resto de marcas y nombres que se mencionan en este documento, puede ser marcas comerciales de las compañías respectivas.

2014 - 12

Rev. A00

Tabla de contenido

1 Descripción general.....15

Novedades de esta versión.....16
Funciones clave.....16
Funciones de administración.....17
Funciones de seguridad.....18
Descripción general del chasis.....18
Versión mínima de CMC.....21
Conexiones de acceso remoto admitidas.....22
Plataformas admitidas.....22
Exploradores web compatibles.....23
Administración de licencias.....23
Tipos de licencias.....23
Adquisición de licencias.....23
Operaciones de licencia.....24
Estado o condición del componente de licencia y operaciones disponibles.....24
Administración de licencias mediante la interfaz web del CMC.....25
Administración de licencias mediante RACADM.....25
Funciones con licencia en el CMC.....25
Visualización de versiones traducidas de la interfaz web del CMC.....27
Aplicaciones admitidas de la consola de administración.....27
Cómo usar esta guía del usuario.....27
Otros documentos que podrían ser de utilidad.....28
Acceso a documentos desde el sitio de asistencia de Dell.....29

2 Instalación y configuración del CMC.....30

Antes de empezar.....30
Instalación de hardware del CMC.....30
Lista de comprobación para configurar el chasis.....30
Conexión básica del CMC a la red.....31
Instalación de software de acceso remoto en una estación de administración.....31
Instalación de RACADM en una estación de administración con Linux.....32
Desinstalación de RACADM desde una estación de administración con Linux.....32
Configuración de un explorador de web.....32
Servidor proxy.....33
Filtro de suplantación de identidad de Microsoft.....33
Obtención de la lista de revocación de certificados.....34
Descarga de archivos desde el CMC con Internet Explorer.....34
Activación de animaciones en Internet Explorer.....34

Configuración del acceso inicial al CMC....34
Configuración inicial de red del CMC....35
Interfaces y protocolos para obtener acceso al CMC....39
Inicio del CMC mediante otras herramientas de Systems Management....41
Descarga y actualización de firmware del CMC....41
Configuración de la ubicación física del chasis y el nombre del chasis....42
Configuración de la ubicación física del chasis y el nombre del chasis mediante la interfaz web....42
Configuración de la ubicación física del chasis y el nombre del chasis mediante RACADM....42
Establecimiento de la fecha y la hora en el CMC....42
Establecimiento de la fecha y la hora en el CMC mediante la interfaz web del CMC....42
Establecimiento de la fecha y la hora en el CMC mediante RACADM....42
Configuración de los LED para identificar componentes en el chasis....43
Configuración del parpadeo de LED mediante la interfaz web del CMC....43
Configuración del parpadeo de LED a través de RACADM....43
Configuración de las propiedades del CMC....44
Configuración del método de inicio del iDRAC con la interfaz web del CMC....44
Configuración del método de inicio de iDRAC con RACADM....44
Configuración de los atributos de la política de bloqueo de inicio de sesión con la interfaz web del CMC....44
Configuración de los atributos de la política de bloqueo de inicio de sesión con RACADM....45
Descripción del entorno de CMC redundante....45
Acerca del CMC en espera....46
Modo a prueba de fallos de CMC....46
Proceso de elección del CMC activo....47
Obtención del estado de condición del CMC redundante....47
Configuración del panel frontal....47
Configuración del botón de encendido....47
Configuración del LCD....48
Acceso a un servidor mediante KVM....48

3 Inicio de sesión en el CMC....50

Acceso a la interfaz web del CMC....50
Inicio de sesión en el CMC como usuario local, usuario de Active Directory o usuario de LDAP....50
Inicio de sesión en el CMC mediante una tarjeta inteligente....51
Inicio de sesión en el CMC mediante el inicio de sesión único....52
Antes de iniciar sesión en el CMC mediante una consola serie, Telnet o SSH....53
Acceso al CMC mediante RACADM....53
Inicio de sesión en el CMC mediante la autentificación de clave pública....53
Varias sesiones en el CMC....54
Cambio de la contraseña de inicio de sesión predeterminada....54

Cambio de la contraseña de inicio de sesión predeterminada mediante la interfaz web..... 55
Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM..... 55
Activación o desactivación del mensaje de advertencia de contraseña predeterminada 55
Activación o desactivación del mensaje de advertencia de contraseña predeterminada mediante la interfaz web.....56
Activación o desactivación del mensaje de advertencia para cambiar la contraseña de inicio de sesión predeterminada mediante RACADM.....56

4 Actualización de firmware..... 57

Descarga de firmware del CMC.....57
Visualización de versiones de firmware actualmente instaladas..... 58
Visualización de versiones de firmware actualmente instaladas mediante la interfaz web del CMC.....58
Visualización de versiones de firmware actualmente instaladas mediante RACADM.....58
Actualización de firmware del CMC.....58
Imagen firmada del firmware del CMC..... 59
Actualización de firmware del CMC mediante la interfaz web.....60
Actualización de firmware del CMC mediante RACADM..... 61
Actualización del firmware de infraestructura del chasis..... 61
Actualización del firmware de infraestructura del chasis mediante la interfaz web del CMC..... 61
Actualización del firmware de la infraestructura del chasis mediante RACADM.....61
Actualización de firmware del iDRAC del servidor..... 62
Actualización de firmware del iDRAC del servidor mediante la interfaz web..... 62
Actualización de firmware de los componentes del servidor.....63
Secuencia de actualización de componentes del servidor.....66
Activación de Lifecycle Controller..... 66
Elección de tipo de actualización de firmware para los componentes del servidor mediante la interfaz web del CMC..... 67
Filtrado de componentes para actualizaciones de firmware..... 67
Visualización del inventario de firmware..... 69
Visualización del inventario de firmware mediante la interfaz web del CMC..... 69
Visualización del inventario de firmware mediante RACADM.....70
Cómo guardar el informe de inventario del chasis mediante la interfaz web del CMC..... 70
Configuración de un recurso compartido de red mediante la interfaz web del CMC.....71
Operaciones de Lifecycle Controller.....71
Reinstalación del firmware de los componentes del servidor..... 72
Reversión del firmware de los componentes del servidor..... 73
Reversión del firmware de los componentes del servidor mediante la interfaz web del CMC..... 73
Actualización de firmware de los componentes del servidor..... 73

Actualización de firmware de los componentes del servidor desde un archivo mediante la interfaz web del CMC....74
Actualización de un solo clic de los componentes del servidor mediante un recurso compartido de red....75
Requisitos previos para utilizar el modo de actualización de recursos compartidos de red....75
Actualización de firmware de los componentes del servidor desde un recurso compartido de red mediante la interfaz web del CMC....76
Eliminación de trabajos programados sobre el firmware de los componentes del servidor....77
Eliminación de trabajos programados sobre el firmware de los componentes del servidor mediante la interfaz web....77
Actualización de los componentes de almacenamiento mediante la interfaz web del CMC....77
Recuperación de firmware del iDRAC mediante el CMC....78

5 Visualización de información del chasis y supervisión de la condición de los componentes y del chasis....79

Visualización de los resúmenes de los componentes y el chasis....79
Gráficos del chasis....80
Información del componente seleccionado....81
Visualización del nombre de modelo del servidor y de la etiqueta de servicio....83
Visualización del resumen del chasis....83
Visualización de información y estado de la controladora del chasis....84
Visualización de información y estado de condición de todos los servidores....84
Visualización de información y estado de condición de un servidor individual....84
Visualización de la información y el estado del módulo de E/S....85
Visualización de información y estado de condición de los ventiladores....85
Configuración de ventiladores....86
Visualización de las propiedades del panel frontal....87
Visualización de información y estado de condición del KVM....87
Visualización de información y condición de la pantalla LCD....88
Visualización de información y estado de condición de los sensores de temperatura....88
Visualización de la capacidad de almacenamiento y el estado de los componentes de almacenamiento....88

6 Configuración del CMC....90

Visualización y modificación de la configuración de red LAN del CMC....90
Visualización y modificación de la configuración de red LAN del CMC mediante la interfaz web del CMC....91
Visualización y modificación de la configuración de red LAN del CMC mediante RACADM....91
Activación de la interfaz de red del CMC....91
Activación o desactivación de DHCP para la dirección de interfaz de red del CMC....92
Activación o desactivación de DHCP para las direcciones IP de DNS....92
Establecimiento de direcciones IP estáticas de DNS....93

Configuración de DNS (IPv4 e IPv6)....93
Configuración de la negociación automática, el modo dúplex y la velocidad de la red (IPv4 e IPv6)....93
Configuración de la unidad de transmisión máxima (MTU) (IPv4 e IPv6)....94
Configuración de las opciones de red y de seguridad de inicio de sesión del CMC....94
Configuración de los atributos de rango de IP con la interfaz web del CMC....94
Configuración de los atributos de rango de IP con RACADM....95
Configuración de las propiedades de la etiqueta LAN virtual para CMC....95
Configuración de las propiedades de la etiqueta LAN virtual para CMC mediante RACADM....96
Configuración de las propiedades de la etiqueta LAN virtual para CMC mediante la interfaz web....96
Configuración de servicios....97
Configuración de los servicios mediante la interfaz web del CMC....97
Configuración de servicios mediante RACADM....98
Configuración de la tarjeta de almacenamiento extendido del CMC....98
Configuración de un grupo de chasis....99
Adición de miembros a un grupo de chasis....99
Eliminación de un miembro del chasis principal....100
Forma de desmontar un grupo de chasis....100
Desactivación de un miembro del chasis miembro....101
Acceso a la página web de un chasis miembro o servidor....101
Propagación de las propiedades del chasis principal al chasis miembro....101
Inventario del servidor para el grupo de MCM....102
Forma de guardar el informe de inventario del servidor....102
Inventario del grupo de chasis y versión de firmware....104
Visualización del inventario del grupo de chasis....104
Visualización del inventario del chasis seleccionado con la interfaz web....104
Visualización de las versiones de firmware de los componentes de servidor seleccionados con la interfaz web....104
Configuración de varios CMC mediante RACADM....105
Creación de un archivo de configuración del CMC....106
Reglas de análisis....107
Modificación de la dirección IP del CMC....108
Visualización y terminación de sesiones en el CMC....109
Visualización y terminación de sesiones en el CMC mediante la interfaz web....109
Visualización y terminación de sesiones en el CMC mediante RACADM....109

7 Configuración de servidores....110

Configuración de nombres de las ranuras....110
Establecimiento de la configuración de red del iDRAC....111
Configuración de los valores de red de QuickDeploy del iDRAC....111
Asignación de dirección IP de QuickDeploy para servidores....114

Modificación de la configuración de red del iDRAC en un servidor individual....114
Modificación de la configuración de red del iDRAC mediante RACADM....115
Configuración de los valores de la etiqueta LAN virtual del iDRAC....115
Configuración de los valores de la etiqueta LAN virtual del iDRAC mediante RACADM....116
Configuración de los valores de la etiqueta LAN virtual del iDRAC mediante la interfaz web....116
Configuración del primer dispositivo de inicio....116
Configuración del primer dispositivo de inicio para varios servidores mediante la interfaz web del CMC....117
Configuración del primer dispositivo de inicio para un servidor individual mediante la interfaz web del CMC....118
Configuración del primer dispositivo de inicio mediante RACADM....118
Configuración de FlexAddress para el servidor....118
Configuración de recurso compartido de archivos remotos....118
Configuración de las opciones de perfil con la replicación de configuración de servidores....119
Acceso a la página Perfiles de servidores....120
Agregar o guardar perfil....120
Aplicación de un perfil....121
Importar archivo....122
Exportar archivo....122
Editar perfil....123
Eliminar perfil....123
Visualizar configuración de perfil....123
Visualización de la configuración de los perfiles almacenados....124
Visualización del registro de perfiles....124
Estado de compleción y solución de problemas....124
Implementación rápida de perfiles....124
Asignación de perfiles del servidor a ranuras....125
Inicio del iDRAC mediante el inicio de sesión único....125
Inicio de la consola remota....127

8 Configuración del CMC para enviar alertas....128
Activación o desactivación de alertas....128
Activación o desactivación de alertas mediante la interfaz web del CMC....128
Filtrado de alertas....128
Configuración de destinos de alerta....129
Configuración de destinos de alerta de las capturas SNMP....129
Configuración de los valores de alertas por correo electrónico....131

9 Configuración de cuentas de usuario y privilegios....134
Tipos de usuarios....134
Modificación de la configuración de cuentas raíz de administración para usuarios....138

Configuración de usuarios locales....139
Configuración de los usuarios locales mediante la interfaz web del CMC....139
Configuración de los usuarios locales mediante RACADM....139
Configuración de usuarios de Active Directory....141
Mecanismos de autentificación compatibles de Active Directory....142
Descripción general del esquema estándar de Active Directory....142
Configuración del esquema estándar de Active Directory....143
Descripción general del esquema extendido de Active Directory....146
Configuración del esquema extendido de Active Directory....148
Configuración de los usuarios LDAP genéricos....157
Configuración del directorio LDAP genérico para acceder a CMC....158
Configuración del servicio de directorio de LDAP genérico mediante la interfaz web del CMC....158
Configuración del servicio de directorio LDAP genérico mediante RACADM....159

10 Configuración del CMC para inicio de sesión único o inicio de sesión mediante tarjeta inteligente....161

Requisitos del sistema....161
Sistemas cliente....162
CMC....162
Prerrequisitos para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente....162
Generación del archivo Keytab de Kerberos....162
Configuración del CMC para el esquema de Active Directory....163
Configuración del explorador para el inicio de sesión único....163
Internet Explorer....163
Mozilla Firefox....164
Configuración de un explorador para el inicio de sesión mediante tarjeta inteligente....164
Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory....164
Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory mediante la interfaz web....164
Carga de un archivo keytab....165
Configuración de inicio de sesión único o inicio de sesión mediante tarjeta inteligente en el CMC para usuarios de Active Directory mediante RACADM....165

11 Configuración del CMC para el uso de consolas de línea de comandos....166

Funciones de la consola de línea de comandos del CMC....166
Comandos para la interfaz de la línea de comandos del CMC....166
Uso de una consola Telnet con el CMC....167
Uso de SSH con el CMC....167
Esquemas de criptografía SSH compatibles....168

Configuración de la autentificación de clave pública en SSH..... 168
Configuración del software de emulación de terminal.....170
Configuración de Minicom de Linux.....171
Conexión a servidores o módulos de E/S con el comando connect.....172
Configuración del BIOS del servidor administrado para la redirección de consola serie.....173
Configuración de Windows para la redirección de consola en serie..... 174
Configuración de Linux para la redirección de la consola en serie del servidor durante el inicio.....174
Configuración de Linux para la redirección de consola serie del servidor después del inicio.....174

12 Uso de las tarjetas FlexAddress y FlexAddress Plus.....176
Acerca de FlexAddress..... 176
Acerca de FlexAddress Plus.....177
Visualización del estado de activación de FlexAddress.....177
Desactivación de FlexAddress.....179
Configuración de FlexAddress.....179
Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis..... 180
Visualización de las direcciones World Wide Name/Media Access Control (WWN/MAC).....181
Configuración de la red Fabric.....181
Visualización de la información de dirección WWN/MAC..... 181
Visualización de información básica sobre la dirección WWN_MAC mediante la interfaz web...183
Visualización de información avanzada sobre la dirección WWN/MAC mediante la interfaz web..... 183
Visualización de información sobre la dirección WWN/MAC mediante RACADM.....184
Mensajes de comandos..... 185
CONTRATO DE LICENCIA DE SOFTWARE DE DELL FlexAddress.....187

13 Administración de redes Fabric..... 190
Situación de encendido por primera vez.....190
Supervisión de la condición del módulo de E/S.....190
Configuración de los valores de red para módulos de E/S.....190
Configuración de los valores de red para los módulos de E/S mediante la interfaz web del CMC..... 191
Configuración de los valores de red para los módulos de E/S mediante RACADM.....191
Administración de la operación de control de alimentación para los módulos de E/S 192
Activación o desactivación del parpadeo del LED para los módulos de E/S 192

14 Administración y supervisión de la alimentación.....193
Políticas de redundancia.....194
Política de redundancia de la red eléctrica.....194
Política de redundancia de suministro de energía.....195

Conexión dinámica de suministros de energía....195
Configuración predeterminada de redundancia....196
Redundancia de cuadrícula....197
Redundancia del suministro de energía....197
Presupuesto de alimentación para módulos de hardware....197
Configuración de la prioridad de alimentación de ranura del servidor....199
Asignación de niveles de prioridad a los servidores....199
Asignación de niveles de prioridad a los servidores mediante la interfaz web del CMC....200
Asignación de niveles de prioridad a los servidores mediante RACADM....200
Visualización del estado del consumo de alimentación....200
Visualización del estado del consumo de alimentación mediante la interfaz web del CMC. 200
Visualización del estado del consumo de alimentación con el comando RACADM....201
Visualización del estado de presupuesto de alimentación mediante la interfaz web del CMC....201
Visualización del estado del presupuesto de alimentación mediante RACADM....201
Estado de redundancia y condición general de la alimentación....201
Administración de la alimentación tras una falla de la unidad de suministro de energía....201
Administración de la alimentación tras la desconexión de una unidad de suministro de energía....202
Política de conexión de servidores nuevos....202
Cambios de suministro de energía y política de redundancia en el registro de sucesos del sistema....204
Configuración de la redundancia y el presupuesto de alimentación....204
Conservación de la energía y presupuesto de alimentación....205
Modo de conservación máxima de energía....205
Reducción de la alimentación del servidor para mantener el presupuesto de alimentación. 205
Operación de unidades de suministro de energía de 110 V....206
Registro remoto....206
Administración de la alimentación externa....206
Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web del CMC....207
Configuración de la redundancia y el presupuesto de alimentación mediante RACADM....207
Ejecución de las operaciones de control de alimentación....209
Ejecución de operaciones de control de alimentación en el chasis....209
Ejecución de operaciones de control de alimentación en el chasis mediante la interfaz web....209
Ejecución de operaciones de control de alimentación en el chasis mediante RACADM....209
Ejecución de operaciones de control de alimentación en un servidor....210
Ejecución de operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC....210
Ejecución de operaciones de control de alimentación en el módulo de E/S....210
Ejecución de operaciones de control de alimentación en módulos de E/S mediante la interfaz web del CMC....210

Ejecución de operaciones de control de alimentación en el módulo de E/S mediante RACADM....211

15 Administración del almacenamiento del chasis....212

Visualización del estado de los componentes de almacenamiento....212
Visualización de la topología de almacenamiento....213
Visualización de la información de solución de problemas con tolerancia a errores de SPERC mediante la interfaz web del CMC....213
Asignación de adaptadores virtuales para ranuras mediante la interfaz web del CMC....214
Tolerancia a errores en las controladoras de almacenamiento....215
Visualización de las propiedades de la controladora mediante la interfaz web del CMC....216
Visualización de las propiedades de las controladoras mediante RACADM....216
Importación o borrado de configuración ajena....216
Configuración de los valores de la controladora de almacenamiento....216
Configuración de los valores de la controladora de almacenamiento mediante la interfaz web del CMC....217
Configuración de los valores de la controladora de almacenamiento mediante RACADM....217
Controladoras PERC compartidas....217
Activación o desactivación de alertas mediante la interfaz web del CMC....218
Activación o desactivación de la controladora RAID mediante RACADM....219
Visualización de las propiedades del disco físico mediante la interfaz web del CMC....219
Visualización de propiedades de unidades de discos físicos mediante RACADM....220
Identificación de discos físicos y discos virtuales....220
Asignación de repuestos dinámicos globales mediante la interfaz web del CMC....220
Asignación de repuestos dinámicos globales mediante RACADM....221
Recuperación de discos físicos....221
Visualización de propiedades de discos virtuales mediante la interfaz web del CMC....221
Visualización de propiedades de discos virtuales mediante RACADM....221
Creación de un disco virtual mediante la interfaz web del CMC....221
Aplicación de la política de acceso para adaptadores virtuales a discos virtuales....222
Modificación de las propiedades de disco virtual mediante la interfaz web del CMC....222
Visualización de las propiedades del gabinete mediante la interfaz web del CMC....223

16 Administración de ranuras PCIe....224

Visualización de propiedades de ranuras PCIe mediante la interfaz web del CMC....224
Asignación de ranuras PCIe a los servidores mediante la interfaz web del CMC....224
Administración de ranuras PCIe mediante RACADM....225
Protección de la alimentación de PCIe....226
Visualización de propiedades de protección de PCIe mediante la interfaz web del CMC....226
Visualización del estado de las propiedades de protección de PCIe mediante RACADM....227
Configuración de las propiedades de protección de PCIe mediante la interfaz web del CMC....227

Configuración del estado de las propiedades de protección de PCIe mediante RACADM.... 227

17 Solución de problemas y recuperación..... 228

Recopilación de información de configuración, estado del chasis y registros mediante RACDUMP..... 228

Interfaces admitidas..... 228

Descarga del archivo MIB (Base de información de administración) SNMP..... 229

Primeros pasos para solucionar problemas de un sistema remoto..... 229

Solución de problemas de alimentación..... 230

Solución de problemas de alertas..... 231

Visualización de los registros de sucesos..... 231

Visualización del registro de hardware..... 232

Visualización del registro del chasis..... 233

Uso de la consola de diagnósticos..... 233

Restablecimiento de componentes..... 233

Guardar o restaurar la configuración del chasis..... 234

Solución de errores de protocolo de hora de red (NTP)..... 234

Interpretación de los colores y los patrones de parpadeo de los LED..... 236

Solución de problemas de un CMC que no responde..... 238

Observación de los LED para aislar el problema..... 238

Obtención de la información de recuperación desde el puerto serie DB-9..... 238

Recuperación de la imagen del firmware..... 239

Solución de problemas de red..... 239

Solución de problemas de la controladora..... 240

18 Uso de la interfaz del panel LCD..... 241

Navegación de la pantalla LCD..... 241

Menú principal..... 242

Menú de asignación de KVM..... 243

Asignación de DVD..... 243

Menú del alojamiento..... 243

Menú Resumen de IP..... 243

Configuración..... 244

Diagnóstico..... 244

Mensajes de la pantalla LCD del panel frontal..... 245

Información de estado del servidor y del módulo de LCD..... 245

19 Preguntas frecuentes..... 252

RACADM..... 252

Administración y recuperación de un sistema remoto..... 253

..... 254

Active Directory..... 254

FlexAddress y FlexAddressPlus..... 255
Módulos de E/S..... 257

1

Descripción general

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

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

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

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

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

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

- El primer dispositivo de inicio en el módulo del servidor
- Las revisiones de congruencia de red Fabric de E/S entre el módulo de E/S y los servidores. El CMC desactiva además componentes, en caso de ser necesario, para proteger el hardware del sistema.
- La seguridad de acceso de los usuarios.
- Los componentes de almacenamiento, incluyendo el modo de tolerancia a errores para las controladoras de almacenamiento.
- Las ranuras de PCIe

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

Novedades de esta versión

Esta versión del CMC para Dell PowerEdge VRTX admite:

- Módulos de servidor de 13.ª generación.

  NOTA: Para obtener más información sobre los servidores correspondientes, consulte la publicación *Dell Chassis Management Controller (CMC) Version 2.00 for Dell PowerEdge VRTX Release Notes* (Notas de versión de Dell Chassis Management Controller (CMC) versión 2.00 para Dell PowerEdge VRTX) disponible en **dell.com/support/home**.
- 1600 W PSU.
- Actualización del firmware de iDRAC y Lifecycle Controller para los servidores de 13.ª generación mediante un solo paquete de firmware del iDRAC.
- Opción para utilizar una biblioteca externa (directorio CIFS/NFS) a fin de actualizar repositorios y perfiles.
- Opción para ver y usar perfiles capturados que estén almacenados en una biblioteca externa.
- Opción para asignar un perfil que esté en una biblioteca a una ranura a fin de implementar rápidamente los perfiles.
- Direcciones IP de QuickDeploy reservadas.
- Capacidad para ver la dirección MAC y el Id. de VLAN del CMC en la pantalla LCD.
- Inventario mejorado de dirección WWN/MAC mediante la función de identidad de E/S del iDRAC.
- Ejecución de la verificación de firmas para los archivos de imagen del firmware del CMC.
- Compatibilidad con NDC Broadcom 1GE de cuatro puertos en el módulo de servidor M630.
- Tarjetas NDC Emulex ARI e intermedias en el módulo de servidor MC630.
- Compatibilidad con 1Gbe y NDC en el módulo de servidor MC630.
- Compatibilidad con NDC habilitados para ARI.

Funciones clave

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

Funciones de administración

El CMC proporciona las siguientes funciones de administración:

- Entorno redundante del CMC.
- Registro del sistema dinámico de nombres de dominio (DDNS) para IPv4 e IPv6.
- Administración y configuración de inicio de sesión para usuarios locales, Active Directory y LDAP.
- Las opciones avanzadas de ventilación como ECM (Modo mejorado de ventilación) y desplazamiento de ventiladores se pueden activar para proporcionar ventilación adicional para un mejor rendimiento.
- Administración y supervisión remotas del sistema por medio de SNMP, una interfaz web, iKVM o una conexión de Telnet o SSH.
- Supervisión: proporciona acceso a la información del sistema y al estado de los componentes.
- Acceso a registros de sucesos del sistema: proporciona acceso al registro de hardware y al registro del chasis.
- Actualizaciones de firmware para diversos componentes del chasis: permite actualizar el firmware para CMC, iDRAC en los servidores, la infraestructura del chasis y el almacenamiento del chasis.
- Actualización de firmware para componentes del servidor, como el BIOS, las controladoras de red, las controladoras de almacenamiento, etc. en varios servidores del chasis con Lifecycle Controller.
- Modo con tolerancia a errores para la SPERC 8 de almacenamiento compartido.
- Integración con el software Dell OpenManage: permite iniciar la interfaz web del CMC desde Dell OpenManage Server Administrator u OpenManage Essentials (OME) 1.2.
- Alerta del CMC: alerta sobre problemas potenciales del nodo administrado mediante un mensaje por correo electrónico de syslog remoto o una captura SNMP.
- Administración remota de la alimentación: proporciona funciones remotas de administración de la alimentación, como el apagado y el restablecimiento de cualquier componente del chasis, desde una consola de administración.
- Informe de uso de la alimentación.
- Cifrado de capa de sockets seguros (SSL): ofrece administración remota y segura de sistemas mediante la interfaz web.
- Punto de inicio para la interfaz web de Integrated Dell Remote Access Controller (iDRAC).
- Compatibilidad con WS-Management.
- Función FlexAddress: reemplaza las direcciones WWN/MAC (Nombre a nivel mundial/Control de acceso a medios) asignadas de fábrica por direcciones WWN/MAC asignadas por el chasis para una ranura particular.
- Compatibilidad con la función de identidad de E/S de iDRAC para mejorar el inventario de direcciones WWN/MAC.
- Gráfico de la condición y el estado de los componentes del chasis.
- Asistencia para servidores simples o de varias ranuras.
- El asistente de configuración iDRAC con LCD admite la configuración de la red del iDRAC.
- Inicio de sesión único de iDRAC.
- Compatibilidad para el protocolo de hora de red (NTP).
- Resumen de servidores, informe de la alimentación y páginas de control de la alimentación mejorados.
- Protección forzada contra fallas del CMC y recolocación virtual de servidores.
- Administración de múltiples chasis donde se permite que hasta otros ocho chasis sean visibles desde el chasis principal.
- Configuración de componentes de almacenamiento en el chasis.

- Asignación de ranuras PCIe a los servidores y su identificación.

Funciones de seguridad

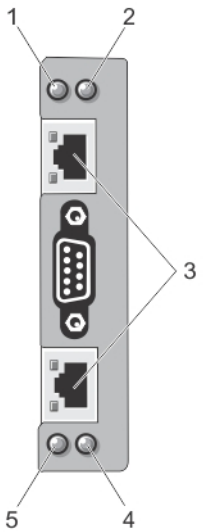
El CMC proporciona las siguientes funciones de seguridad:

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

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

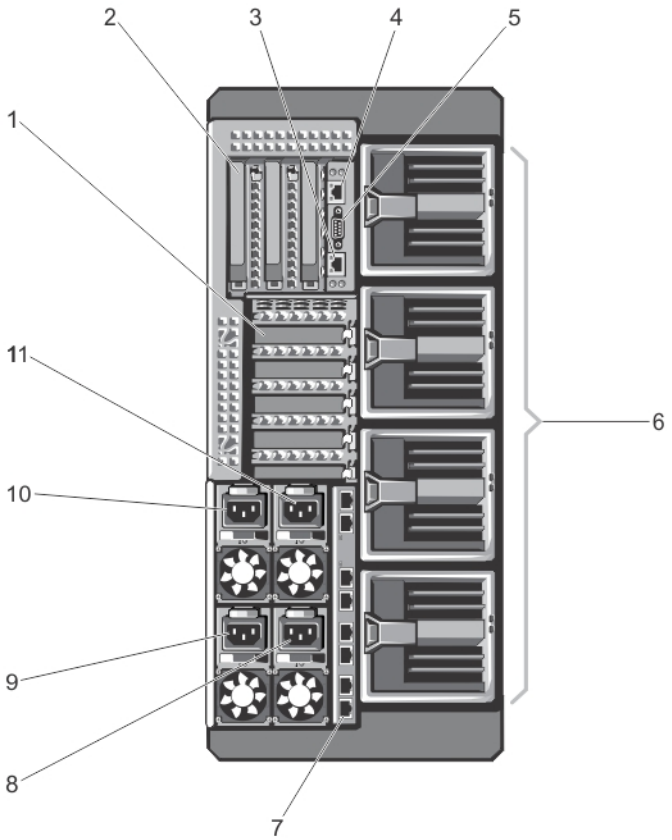
Descripción general del chasis

Esta figura muestra una vista de los conectores del CMC.



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

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



Elemento	Indicador, botón o conector
1	Ranuras de tarjetas de expansión PCIe de perfil bajo (5)
2	Ranuras para tarjeta de expansión PCIe de altura completa (3)
3	Puerto GB Ethernet del CMC (CMC-2)

Elemento	Indicador, botón o conector
4	Puerto GB Ethernet del CMC (CMC-1)
5	Conector serie
6	Módulos de ventilación (4)
7	Puertos del módulo de E/S
8	PSU 4
9	PSU 3
10	PSU 1
11	PSU 2

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

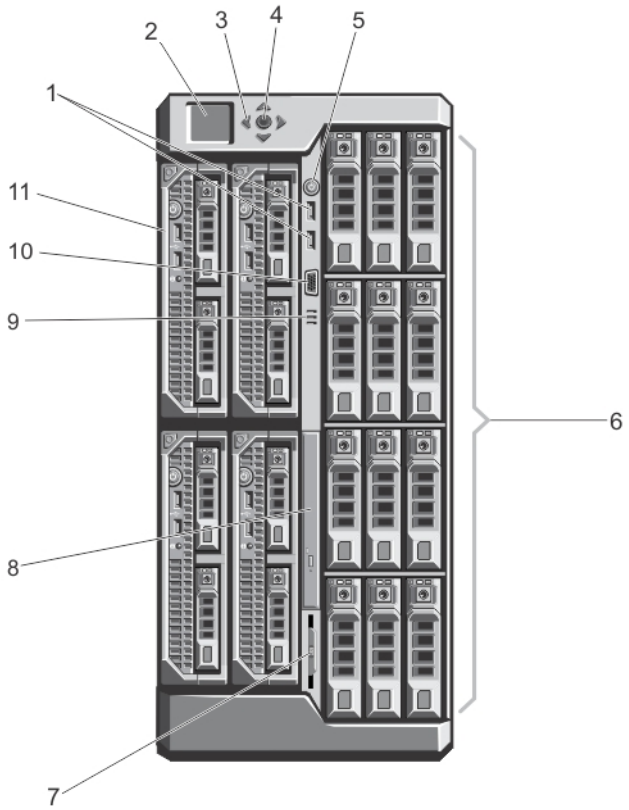


Ilustración 1. Características e indicadores del panel frontal: chasis de la unidad de disco duro de 3,5 pulgadas

Elemento	Indicador, botón o conector	Descripción
1	Conectores USB (2)	Permite conectar un teclado y un mouse al sistema.
2	Panel LCD	Proporciona información sobre el sistema y su estado, así como mensajes de error para indicar que el sistema funciona correctamente o que se requiere atención.
3	Botones de desplazamiento del menú del LCD (4)	Desplaza el cursor en incrementos de un paso.
4	Botón de selección ("check")	Selecciona y guarda un elemento en la pantalla LCD y avanza a la pantalla siguiente.
5	Indicador de encendido, botón de encendido del gabinete	El indicador de encendido se ilumina cuando la alimentación del gabinete está activada. El botón de encendido controla la unidad de suministro de energía (U.S.E) de salida al sistema.
6	Unidades de disco duro	**Gabinete de unidades de disco duro de 2,5 pulgadas**: Hasta 25 unidades de disco duro de intercambio activo de 2,5 pulgadas. **Gabinete de unidades de disco duro de 3,5 pulgadas**: Hasta 12 unidades de disco duro de intercambio activo de 3,5 pulgadas.
7	Etiqueta de información	Panel de etiquetas de deslizamiento que permite registrar información del sistema, como la etiqueta de servicio, la NIC, la dirección MAC, la clasificación eléctrica del sistema y las marcas de las agencias reguladoras de todo el mundo.
8	Unidad óptica (opcional)	Una unidad de DVD-ROM SATA o DVD+/-RW opcional.
9	Rejillas de ventilación	Rejillas de ventilación para el sensor de temperatura. **NOTA:** Para asegurarse de que el enfriamiento sea adecuado, verifique que las rejillas de ventilación no estén bloqueadas.
10	Conector de video	Permite conectar un monitor al sistema.
11	Módulos del servidor	Hasta cuatro módulos de servidor PowerEdge M520, M620 o M630, o bien, 2 módulos de servidor M820 específicamente configurados para el gabinete.

Versión mínima de CMC

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

Tabla 1. Versión mínima de CMC para los módulos del servidor

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

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

Tabla 2. Versión mínima de CMC para los módulos de E/S

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

Conexiones de acceso remoto admitidas

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

Tabla 3. Conexiones de acceso remoto admitidas

Conexión	Características
Puertos de la interfaz de red del CMC	• Puerto GB: interfaz de red dedicada para la interfaz web del CMC • Compatibilidad con DHCP. • Notificación de sucesos por correo electrónico y capturas SNMP • Interfaz de red para el iDRAC y los módulos de E/S (IOM). • Compatibilidad con la consola de comandos Telnet/SSH y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado del sistema.
Puerto serie	• Compatibilidad con la consola serie y los comandos de CLI de RACADM, incluso los comandos de inicio, restablecimiento, encendido y apagado del sistema. • Compatibilidad con el intercambio binario para aplicaciones diseñadas específicamente para comunicarse mediante un protocolo binario con un tipo particular de módulo de E/S. • El puerto serie se puede conectar internamente a la consola serie de un servidor, o un módulo de E/S, mediante el comando connect (o racadm connect). • Proporciona acceso solamente al CMC activo

Plataformas admitidas

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

Para obtener información sobre las plataformas más recientes, consulte *Dell Chassis Management Controller (CMC) Version 2.00 for Dell PowerEdge VRTX Release Notes* (Notas de versión de Dell Chassis

Management Controller (CMC) versión 2.00 para Dell PowerEdge VRTX) disponible en **dell.com/support/manuals**.

Exploradores web compatibles

Dell PowerEdge VRTX admite los siguientes exploradores web:

- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 11
- Safari versión 6.0
- Safari versión 7.0
- Mozilla Firefox versión 29
- Mozilla Firefox versión 30
- Google Chrome versión 33
- Google Chrome versión 34

Administración de licencias

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

Tipos de licencias

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

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

Adquisición de licencias

Utilice cualquiera de los métodos siguientes para adquirir licencias:

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

Operaciones de licencia

Antes de poder realizar las tareas de administración de licencias, asegúrese de adquirir las licencias necesarias. Para obtener más información, consulte la Overview and Feature Guide (Guía de información general y funciones) disponible en support.dell.com.

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

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

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

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

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

Estado o condición del componente de licencia y operaciones disponibles

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

Tabla 1. Operaciones de licencia según el estado y la condición

Estado o condición de la licencia o el componente	Import	Exportar	Eliminar	Reemplazar	Más información
Inicio de sesión no de administrador	No	Sí	No	No	Sí

Licencia activa	Sí	Sí	Sí	Sí	Sí
Licencia caducada	No	Sí	Sí	Sí	Sí
Licencia instalada pero falta el componente	No	Sí	Sí	No	Sí

Administración de licencias mediante la interfaz web del CMC

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

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

La página **Licencias** muestra las licencias asociadas a los dispositivos o las licencias instaladas pero para las que no hay dispositivos presentes en el sistema. Para obtener más información sobre la importación, exportación, eliminación o sustitución de licencias consulte la *ayuda en línea*.

Administración de licencias mediante RACADM

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

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

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

Funciones con licencia en el CMC

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

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

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

Configuración avanzada	No	Sí	
Copia de seguridad a nivel de gabinete	No	Sí	
Activación de FlexAddress	No*	Sí	*Para la configuración no predeterminada de FlexAddress, solo se admite la función Restaurar valores predeterminados con la licencia Express. Restaurar valores predeterminados restablecerá la dirección Flex a los valores predeterminados de fábrica.
Asignación de adaptador de PCIe	Sí*	Sí	*Se puede asignar un máximo de dos adaptadores de PCIe por servidor con la licencia Express.
Adaptador virtual para la asignación de ranuras	No*	Sí	*Para la asignación no predeterminada del Adaptador virtual, solo se admite la función Asignación predeterminada con la licencia Express. Restaurar valores predeterminados cambiará la asignación del adaptador virtual a los valores predeterminados de fábrica.
Adaptador virtual para desasignación de ranuras	Sí	Sí	
Clonación de servidores	No	Sí	
Actualización de firmware del servidor de uno a muchos	No	Sí	
Configuración de uno a muchos para iDRAC	No	Sí	

Visualización de versiones traducidas de la interfaz web del CMC

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

Aplicaciones admitidas de la consola de administración

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

Cómo usar esta guía del usuario

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

- La interfaz web: aquí solo se proporciona información relacionada con las tareas. Para obtener información sobre los campos y las opciones, consulte *CMC for Dell PowerEdge VRTX Online Help (Ayuda en línea del CMC para Dell PowerEdge VRTX)* que se puede abrir desde la interfaz web.

- Los comandos RACADM: aquí se proporciona el comando RACADM o el objeto que se debe utilizar. Para obtener más información sobre un comando RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en dell.com/support/manuals.

Otros documentos que podrían ser de utilidad

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

- En *VRTX CMC Online Help* (Ayuda en línea del CMC para VRTX) se ofrece información acerca de cómo usar la interfaz web. Para acceder a la ayuda en línea, haga clic en **Ayuda** en la interfaz web del CMC.
- En *Chassis Management Controller Version 2.0 for Dell PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller versión 2.0 para Dell PowerEdge VRTX) se proporciona información sobre cómo usar las funciones RACADM relacionadas con VRTX.
- En *Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX Version 2.00 Release Notes* (Notas de publicación de Dell Chassis Management Controller (CMC) para Dell PowerEdge VRTX versión 2.00) se proporcionan actualizaciones de último minuto para el sistema, así como documentación o material de referencia con información técnica sobre opciones avanzadas para técnicos o usuarios experimentados.
- En *Integrated Dell Remote Access Controller (iDRAC) User's Guide* (Guía del usuario de Integrated Dell Remote Access Controller [iDRAC]), se ofrece información sobre la instalación, la configuración y el mantenimiento del iDRAC en sistemas administrados.
- En *Dell OpenManage Server Administrator's User's Guide (Guía del usuario de Dell OpenManage Server Administrator)*, se proporciona información sobre la forma de instalar y utilizar Server Administrator.
- En *Dell Update Packages User's Guide (Guía del usuario de Dell Update Packages)*, se brinda información sobre la forma de obtener y usar Dell Update Packages como parte de la estrategia de actualización del sistema.
- La *Dell Shared PowerEdge RAID Controller (PERC) 8 User's Guide* (Guía del usuario de la Controladora Dell PowerEdge RAID (PERC) 8 compartida) proporciona información acerca de la implementación de la tarjeta PERC 8 compartida y la administración del subsistema de almacenamiento. Este documento está disponible en línea en **dell.com/storagecontrollermanuals**.
- En la documentación de la aplicación de administración de sistemas Dell se proporciona información sobre cómo instalar y utilizar el software de administración de sistemas.

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

- Las instrucciones de seguridad incluidas con el sistema proporcionan información importante sobre la seguridad y las normativas. Para obtener más información sobre las normativas, consulte la página de inicio de cumplimento normativo en **www.dell.com/regulatory_compliance**. Es posible que se incluya información de garantía en este documento o en un documento separado.
- En *Dell PowerEdge VRTX Getting Started Guide* (Guía de introducción a Dell PowerEdge VRTX) que se envía con el sistema se ofrece una descripción general de las funciones del sistema, de la configuración del sistema y de las especificaciones técnicas.
- En el placemat de configuración que se envía con el sistema se ofrece información sobre la instalación y la configuración iniciales del sistema.
- En el *manual del propietario* del módulo del servidor se ofrece información acerca de las funciones del módulo del servidor y se describe cómo solucionar los problemas en el módulo del servidor e instalar o reemplazar los componentes del módulo del servidor. Este documento está disponible en línea en **dell.com/poweredgemanuals**.

- En la documentación del bastidor incluida con la solución del bastidor se describe cómo instalar el sistema en un bastidor, si es necesario.
- Para ver el nombre completo de las abreviaturas o siglas utilizadas en este documento, consulte Glossary (Glosario) en **dell.com/support/manuals**.
- En la documentación del software de administración de sistemas se describen las características, los requisitos, la instalación y el funcionamiento básico del software.
- En la documentación de los componentes adquiridos por separado se incluye información para configurar e instalar las opciones correspondientes.
- Todos los medios que se envían con el sistema y que proporcionan documentación y herramientas para configurar y administrar el sistema, incluyendo los medios relacionados con el sistema operativo, el software de administración del sistema, las actualizaciones del sistema y los componentes del sistema adquiridos con el sistema. Para obtener más información sobre el sistema, busque la herramienta Quick Resource Locator (QRL) disponible en el sistema y el placemat de configuración del sistema que se envía con el sistema. Descargue la aplicación QRL desde la plataforma móvil para activarla en el dispositivo móvil.

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

Acceso a documentos desde el sitio de asistencia de Dell

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

- Mediante los siguientes enlaces:
  - Para todos los documentos de Enterprise Systems Management: **dell.com/softwaresecuritymanuals**
  - Para documentos de Enterprise System Management: **dell.com/openmanagemanuals**
  - Para documentos de Remote Enterprise System Management: **dell.com/esmmanuals**
  - Para documentos de OpenManage Connections Enterprise Systems Management: **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Para documentos de Herramientas de servicio: **dell.com/serviceabilitytools**
  - Para documentos de Client Systems Management: **dell.com/clientsystemsmanagement**
  - Para documentos de OpenManage Connections Client Systems Management: **dell.com/connectionsclientsystemsmanagement**
- En el sitio web de asistencia de Dell:
  a. Vaya a **dell.com/support/home**.
  b. En la sección **Asistencia general**, haga clic en **Software y seguridad**.
  c. En el grupo **Software y seguridad**, haga clic en el vínculo requerido que corresponda:
     - **Administración de sistemas Enterprise**
     - **Administración remota de sistemas Enterprise**
     - **Herramientas de servicio**
     - **Administración de sistemas cliente**
     - **Administración de conexiones de sistemas cliente**
  d. Para ver un documento, haga clic en la versión del producto requerida.
- Mediante los motores de búsqueda:
  - Escriba el nombre y la versión del documento en el cuadro buscar.

2

Instalación y configuración del CMC

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

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

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

Antes de empezar

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

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

Instalación de hardware del CMC

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

Lista de comprobación para configurar el chasis

Las siguientes tareas permiten configurar el chasis con precisión:

1. El CMC y la estación de administración donde se utiliza el explorador deben estar en la misma red, la cual se denomina red de administración. Conecte un cable de red Ethernet del puerto del CMC activo a la red de administración.
2. Instale el módulo de E/S en el chasis y conecte el cable de red al chasis.
3. Inserte los servidores en el chasis.
4. Conecte el chasis a la fuente de alimentación.
5. Presione el botón de encendido o encienda el chasis desde la interfaz web del CMC después de completar la tarea en el paso 7.

   NOTA: No encienda los servidores.
6. Mediante el panel LCD, navegue hasta el resumen de IP y haga clic en el botón de selección "Check"(Verificar). Use la dirección IP del CMC en el explorador del sistema de administración (E/S,

Chrome o Mozilla). Para configurar DHCP para el CMC, use el panel LCD para hacer clic en **Menú principal → Configuración → Configuración de red**.

7. Conecte a la dirección IP del CMC mediante un explorador web al escribir el nombre de usuario predeterminado (root) y la contraseña (calvin).
8. Proporcione una dirección IP a cada iDRAC en la interfaz web del CMC y active la interfaz LAN e IPMI.

   NOTA: De forma predeterminada, la interfaz LAN de iDRAC en algunos servidores está desactivada. Esta información se puede encontrar en la interfaz web del CMC en **Descripción general del servidor → Configuración**. Esta puede ser una opción de licencia avanzada, en cuyo caso se debe usar la función **Configuración** para cada servidor).
9. Proporcione el módulo de E/S con una dirección IP en la interfaz web del CMC. Es posible obtener la dirección IP al hacer clic en **Descripción general del módulo de E/S** y, a continuación, haga clic en **Configuración**.
10. Conecte cada iDRAC a través del explorador web y proporcione la configuración final del iDRAC. De forma predeterminada, el nombre de usuario es `root` y la contraseña es `calvin`.
11. Conecte el módulo de E/S mediante el explorador web y proporcione la configuración final del módulo de E/S.
12. Encienda los servidores e instale el sistema operativo.

Conexión básica del CMC a la red

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

Instalación de software de acceso remoto en una estación de administración

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

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

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

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

Instalación de RACADM en una estación de administración con Linux

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

   NOTA: En el sistema operativo Red Hat Enterprise Linux 5, los DVD se montan automáticamente mediante la opción `–noexec mount`. Esta opción no permite ejecutar ningún archivo ejecutable desde el DVD. Es necesario montar el DVD-ROM manualmente y, a continuación, ejecutar los comandos.
4. Desplácese hasta el directorio **SYSMGMT/ManagementStation/linux/rac**. Para instalar el software RAC, escriba el siguiente comando:

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

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

Desinstalación de RACADM desde una estación de administración con Linux

1. Inicie sesión como `root` en el sistema en el que desea desinstalar las funciones de Management Station.
2. Use el siguiente comando de consulta rpm para determinar qué versión de DRAC Tools está instalada.

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

Configuración de un explorador de web

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

El CMC y la Management Station desde donde se utiliza el explorador deben encontrarse en la misma red, que se denomina *red de administración*. En función de los requisitos de seguridad personales, la red de administración puede ser una red aislada y altamente segura.

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

Algunas funciones de los exploradores pueden interferir con la conectividad o el rendimiento, especialmente si la red de administración no tiene una ruta a Internet. Si la estación de administración

ejecuta un sistema operativo Windows, algunas configuraciones de Internet Explorer pueden interferir con la conectividad, incluso cuando se utiliza una interfaz de línea de comandos para obtener acceso a la red de administración.

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

Servidor proxy

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

Internet Explorer

Para editar la lista de excepciones en Internet Explorer:

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

Mozilla Firefox

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

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

Filtro de suplantación de identidad de Microsoft

Si se activa el filtro de suplantación de identidad (phishing) de Internet Explorer en el sistema de administración y el CMC no tiene acceso a Internet, el acceso al CMC puede demorarse unos segundos. Esta demora puede ocurrir si se utiliza el explorador u otra interfaz como RACADM remoto. Realice estos pasos para desactivar el filtro de suplantación de identidad:

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

Obtención de la lista de revocación de certificados

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

Para desactivar la obtención de la CRL:

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

Descarga de archivos desde el CMC con Internet Explorer

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

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

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

Activación de animaciones en Internet Explorer

Cuando se transfieren archivos hacia y desde la interfaz web, un icono de transferencia de archivos gira para mostrar la actividad de transferencia. Mientras se utilice Internet Explorer, se debe configurar el explorador para reproducir animaciones.

Para configurar Internet Explorer para reproducir animaciones:

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

Configuración del acceso inicial al CMC

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

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

Para obtener información sobre la configuración de los valores de red del CMC, consulte Configuring Initial CMC Network (Configuración inicial de red del CMC). Esta configuración inicial asigna los parámetros de red TCP/IP que permiten obtener acceso al CMC.

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

El CMC se conecta a la red de administración. Todo el acceso externo al CMC y a los iDRAC se realiza mediante el CMC. Recíprocamente, el acceso a los servidores administrados se realiza mediante conexiones de red a los módulos de E/S. Esto permite aislar la red de aplicaciones de la red de administración.

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

Configuración inicial de red del CMC

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

La configuración inicial de red del CMC se puede realizar antes o después de asignar una dirección IP al CMC. Si se establece la configuración inicial de red del CMC antes de tener una dirección IP, se puede utilizar cualquiera de las siguientes interfaces:

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

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

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

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

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

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

NOTA: Es posible personalizar la orientación de una pantalla LCD (para los modos de bastidor o torre). Para hacerlo, mantenga presionados los botones de encendido/apagado durante 2 segundos. De forma alternativa, también puede usar los botones de la derecha o izquierda. Para obtener más información acerca de los botones disponibles en el panel LCD del CMC, consulte LCD Navigation (Navegación de la pantalla LCD).

:

1. Para iniciar la configuración del CMC:
   - En el caso de un chasis que no se ha configurado anteriormente, aparece el panel **Idioma de LCD**. En el panel **Idioma de LCD**, vaya al idioma necesario mediante el uso de los botones de flecha. Cuando se resalta el idioma deseado, para seleccionar el idioma presione el botón del centro. Aparece el panel **Configuración de red**.
   - En el caso de un chasis que se ha configurado anteriormente, aparece el panel **Menú principal**. En **Menú principal**, seleccione **Configuración** y, a continuación, **Configuración de red**.
2. En el panel **Configuración de red**, seleccione el modo de configuración requerido:
   - **Configuración rápida (DHCP)**: seleccione este modo para configurar el CMC rápidamente mediante las direcciones de DHCP. Para obtener información sobre la forma de configurar el CMC por medio de este modo, consulte **Configuración del CMC mediante la Configuración rápida (DHCP)**.
   - **Configuración avanzada**: seleccione este modo para configurar las opciones avanzadas del CMC. Para obtener información sobre la forma de configurar el CMC por medio de este modo, consulte **Configuración del CMC mediante la Configuración avanzada**.

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

Para configurar una red mediante la interfaz del panel LCD:

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

   ```
   About to get DHCP addresses. Ensure CMC network cable is connected.
   ```
2. Presione el botón central para resaltar el botón aceptar. Presione el botón central nuevamente para confirmar la configuración o desplácese hasta la flecha posterior y presione el botón central para regresar y modificar la configuración.

Configuración avanzada del CMC

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

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

   NOTA: Para omitir la configuración del CMC, vaya al icono 'X' y presione el botón central.
3. Si el sistema le solicita que seleccione una velocidad de la red adecuada, seleccione una velocidad de la red (**Negociación automática (1 Gb)**,**10 Mb** o **100 Mb**) con los botones correspondientes.

   Para lograr un rendimiento efectivo de la red, el valor de la velocidad de la red debe coincidir con la configuración de la red. Si la velocidad de la red se configura con un valor inferior al de la configuración de la red, aumenta el consumo de ancho de banda y ralentiza la comunicación de la red. Determine si la red admite las velocidades mencionadas arriba y realice la configuración

adecuada. Si la configuración de la red no coincide con ninguno de estos valores, se recomienda seleccionar la opción **Negociación automática (1 Gb)** o consulte la documentación para el usuario del fabricante del equipo de red.

4. Realice una de las siguientes tareas:
   - Seleccione **Negociación automática (1 Gb)** pulsando el botón central y, a continuación, presione el botón central nuevamente. Aparece el panel **Protocolo**. Vaya al paso 6.
   - Seleccione **10 Mb** o **100 Mb**. El panel **Dúplex**

     aparece. Vaya al paso 5.

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

   NOTA: La configuración del modo dúplex y de la velocidad de la red no están disponibles si la opción **Negociación automática** está establecida en **Activada** o si está seleccionada la opción **1000 MB (1 Gbps)**. Si la negociación automática está activada 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, se selecciona dúplex medio como el modo dúplex durante la negociación automática. Esta incompatibilidad del modo dúplex hace que la conexión de la red sea lenta.
6. En el panel **Protocolo**, seleccione el protocolo de Internet (**Solo IPv4**, **Solo IPv6** o **Ambos**) que desea utilizar para el CMC, presione el botón central y, a continuación, vuelva a presionar el mismo botón.
7. - Si selecciona **IPv4** o **Ambos**, seleccione modo **DHCP** o **Estático** . Vaya al paso 8.
   - De lo contrario, si selecciona **IPv6**, aparecerá el panel **Configurar iDRAC**. Vaya al paso 11 más adelante en este procedimiento.
8. En el panel **Modo**, seleccione el modo en el cual el CMC debe obtener las direcciones IP de NIC. Si selecciona DHCP, CMC recupera la configuración IP (dirección IP, máscara y puerta de enlace) automáticamente desde un servidor DHCP en la red. Al CMC se le asigna una dirección IP exclusiva que se distribuye en la red. Si selecciona **DHCP**, presione el botón central y, a continuación, vuelva a presionar el mismo botón. Aparece el panel **Configurar iDRAC**. Vaya al paso 11 más adelante en este procedimiento.
9. Si selecciona **Estática**, introduzca la dirección IP, la puerta de enlace y la máscara de subred de acuerdo con las instrucciones en el panel LCD.

   Se muestra la información IP que introdujo. Presione el botón central y, a continuación, vuelva a presionar el mismo botón. La pantalla **Configuración de CMC** muestra la configuración de la **dirección IP estática**, la **máscara de subred** y la **puerta de enlace** que ha introducido. Compruebe la configuración para asegurarse de su precisión. Para corregir un valor, presione los botones correspondientes. Presione el botón central y, a continuación, presione nuevamente el mismo botón. Aparece el panel **¿Registrar DNS?**
10. Para registrar seleccione el icono de verificación y presione el botón central. Establezca la dirección IP de DNS, seleccione el icono de verificación y, a continuación, presione el botón central. Si el registro de DNS no es necesario, a continuación, seleccione este icono 'X' y presione el botón central.
11. Indique si desea o no configurar iDRAC:
    - **No**: seleccione el icono 'X' y, a continuación, presione el botón central. Vaya al paso 17 más adelante en este procedimiento.
    - **Sí**: seleccione el icono de verificación y, a continuación, presione el botón central.

También puede configurar iDRAC desde la interfaz web del CMC.

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

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

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

      : aparece el panel **Configuración del iDRAC**. Vaya al paso 15.

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

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

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

14. En el panel **IPMI en la LAN**, seleccione **Activar** o **Desactivar** para activar o desactivar la IPMI en la LAN. Presione el botón central para continuar.
15. En el panel **Configuración de iDRAC** se muestra el siguiente mensaje.
    `Apply settings to installed servers?`

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

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

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

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

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

    `Apply All Enclosure Settings?`

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

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

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

    El CMC y los iDRAC ahora están disponibles en la red. Puede obtener acceso al CMC en la dirección IP asignada por medio de la interfaz web o las interfaces de línea de comandos, por ejemplo, una consola serie, Telnet y SSH.

Interfaces y protocolos para obtener acceso al CMC

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

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

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

Tabla 4. Interfaces del CMC

Interfaz	Descripción
Interfaz web	Proporciona acceso remoto al CMC por medio de una interfaz gráfica de usuario. La interfaz web está incorporada en el firmware del CMC y se puede obtener acceso a ella por medio de la interfaz del NIC desde un explorador web compatible en la estación de administración. Para obtener una lista de los exploradores web compatibles, consulte la sección correspondiente en *Dell System Software Support Matrix* (Matriz

Interfaz	Descripción
	de compatibilidad de software de los sistemas Dell) en **dell.com/support/manuals**.
Interfaz de línea de comandos de RACADM remoto	Use esta utilidad de línea de comandos para administrar el CMC y sus componentes. Puede usar el RACADM de firmware o el RACADM remoto: • El RACADM remoto es una utilidad cliente que se ejecuta en una estación de trabajo. Utiliza la interfaz de red fuera de banda para ejecutar los comandos RACADM en los sistemas administrados y utiliza el canal HTTPS. La opción `–r` ejecuta el comando RACADM sobre una red. • Se puede obtener acceso al RACADM de firmware cuando se inicia sesión en el CMC mediante SSH o Telnet. Es posible ejecutar los comandos de RACADM de firmware sin especificar el nombre de usuario, la contraseña o la dirección IP del CMC. Después de introducir los valores necesarios en la petición de RACADM, es posible ejecutar directamente los comandos sin el prefijo racadm.
Panel LCD del chasis	Use la pantalla LCD en el panel frontal para realizar lo siguiente: • Visualizar alertas e IP del CMC. • Configure DHCP. • Configure los valores de dirección IP estática del CMC. • Ver la dirección MAC del CMC activo. • Ver el Id. de VLAN del CMC que se agrega al final de la dirección IP del CMC, si ya se ha configurado la VLAN.
Telnet	Proporciona acceso de la línea de comandos al CMC a través de la red. La interfaz de línea de comandos RACADM y el comando `connect`, que se utiliza para conectar a la consola serie de un servidor o módulo de E/S, están disponibles desde la línea de comandos del CMC. **NOTA:** Telnet no es un protocolo seguro y está desactivado de manera predeterminada. Telnet transmite todos los datos, incluidas las contraseñas, en texto sin formato. Al transmitir información confidencial, utilice la interfaz SSH.
SSH	Use SSH para ejecutar comandos RACADM. Esto proporciona las mismas capacidades que la consola Telnet, pero utiliza una capa de transporte cifrada para aumentar la seguridad. El servicio SSH está activado de forma predeterminada en el CMC y se puede desactivar.
WS-MAN	Los servicios WSMAN se basan en el protocolo Web Services for Management (WSMAN) para realizar tareas de administración de uno a varios sistemas. Debe utilizar el cliente WS-MAN como cliente WinRM (Windows) o cliente OpenWSMAN (Linux) para utilizar la funcionalidad Servicios remotos LC. También puede utilizar Power Shell y Python para crear secuencias de comandos para la interfaz WS-MAN. WSMAN es un protocolo basado en el protocolo simple de acceso a objetos (SOAP) que se utiliza para la administración de sistemas. El CMC usa WS–Management para transmitir información de administración basada en el modelo común de información (CIM) para el grupo de

Interfaz	Descripción
	trabajo de administración distribuida (DMTAF). La información CIM define la semántica y los tipos de datos que se pueden modificar en un sistema administrado. La implementación WS-MAN del CMC usa SSL en el puerto 443 para la seguridad de transporte y admite la autentificación básica. Los datos disponibles a través de WS-Management se proporcionan con la interfaz de instrumentación del CMC asignada a los perfiles de DMTF y los perfiles de extensión. Para obtener más información, ver: • MOF y perfiles: **delltechcenter.com/page/DCIM.Library** • Sitio web de DTMF: **dmtf.org/standards/profiles/** • Archivo de WS-MAN Release notes. • **www.wbemsolutions.com/ws_management.html** • Especificaciones DMTF para WS-Management: **www.dmtf.org/standards/wbem/wsman** Las interfaces de servicios web pueden utilizarse aprovechando la infraestructura cliente, como Windows WinRM y Powershell CLI, utilidades de código fuente abierto como WSMANCLI y entornos de programación de aplicaciones como Microsoft .NET. Para establecer una conexión de cliente mediante Microsoft WinRM, la versión mínima requerida es 2.0. Para obtener más información, consulte el artículo de Microsoft, <**support.microsoft.com/kb/968929**>.

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

Inicio del CMC mediante otras herramientas de Systems Management

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

Para obtener acceso a la interfaz del CMC mediante Dell Server Administrator, inicie Server Administrator en la estación de administración. En el panel izquierdo de la página de inicio de Server Administrator, haga clic en **Sistema → Chasis del sistema principal → Remote Access Controller**. Para obtener más información, consulte *Dell Server Administrator User's Guide* (Guía del usuario de Dell Server Administrator) en **dell.com/support/manuals**.

Descarga y actualización de firmware del CMC

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

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

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

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

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

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

1. En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Configuración**.
2. En la página **Configuración general del chasis**, escriba las propiedades de la ubicación y el nombre del chasis. Para obtener más información acerca de las propiedades de configuración del chasis, consulte *CMC Online Help* (Ayuda en línea del CMC).

   NOTA: El campo **Ubicación del chasis** es opcional. Se recomienda usar los campos **Centro de datos**, **Pasillo**, **Bastidor** y **Ranura de bastidor** para indicar la ubicación física del chasis.
3. Haga clic en **Aplicar**. Se guardará la configuración.

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

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

Establecimiento de la fecha y la hora en el CMC

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

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

Para establecer la fecha y hora en el CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Configuración** → **Fecha/Hora**.
2. Para sincronizar la fecha y la hora con un servidor de protocolo de tiempo de red (NTP), vaya a la página **Fecha/Hora**, seleccione **Activar NTP** y especifique hasta tres servidores NTP. Para establecer manualmente la fecha y la hora, desactive la opción **Activar NTP** y, a continuación, edite los campos **Fecha** y **Hora**.
3. Seleccione la **zona horaria** en el menú desplegable y haga clic en **Aplicar**.

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

Para establecer la fecha y la hora con la interfaz de la línea de comandos, consulte las secciones de grupo de propiedades de base de datos `fgRemoteHosts` y del comando **config** en *Chassis Management*

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

Configuración de los LED para identificar componentes en el chasis

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

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

Configuración del parpadeo de LED mediante la interfaz web del CMC

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

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

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

    NOTA: Solo se pueden seleccionar unidades de discos físicos y discos virtuales en esta página.

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

Configuración del parpadeo de LED a través de RACADM

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

`racadm setled -m <module> [-l <ledState>]`, donde `<module>` especifica el módulo del LED que desea configurar. Opciones de configuración:

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

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

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

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

Configuración de las propiedades del CMC

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

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

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

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

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

Configuración del método de inicio de iDRAC con RACADM

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

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

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

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

1. En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Red** → **Red**.
   Aparecerá la página **Configuración de red**.
2. En la sección Configuración de IPv4, haga clic en **Opciones avanzadas**. De manera alternativa, para acceder a la página **Seguridad de inicio de sesión**, en el panel izquierdo, en **Descripción general del chasis**, haga clic en **Seguridad** → **Inicio de sesión**.
   Aparecerá la página **Seguridad de inicio de sesión**.

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

   Se activarán las opciones para configurar los otros atributos de la política de bloqueo de inicio de sesión.
4. Introduzca los valores requeridos de los atributos de la política de bloqueo de inicio de sesión en los campos activados: **Bloqueo por conteo de intentos fallidos**, **Ventana de bloqueo por intentos fallidos** y **Bloqueo por tiempo de penalidad**. Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
5. Para guardar estas opciones, haga clic en **Aplicar**.

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

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

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

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

Descripción del entorno de CMC redundante

Puede instalar un CMC en espera que asume la administración si el CMC activo deja de funcionar. El CMC redundante puede estar ya instalado o se puede instalar posteriormente. Para garantizar redundancia completa o el mejor rendimiento, es importante que la red del CMC esté conectada correctamente

Las protecciones contra fallas pueden ocurrir cuando:

- Ejecute el comando `cmcchangeover` de RACADM. Consulte la sección del comando `cmcchangeover` en *Chassis Management Controller for PowerEdge VRTX RACADM Command Line*

Reference Guide (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX) disponible en dell.com/support/manuals.

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

NOTA: En caso de una protección contra fallas en el CMC, se cerrarán todas las conexiones del iDRAC y todas las sesiones activas del CMC. Los usuarios con sesiones cerradas deberán volver a conectarse al nuevo CMC activo.

Acerca del CMC en espera

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

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

NOTA: Para obtener información sobre cómo instalar un CMC, consulte *VRTX Owner's Manual (Manual del propietario de VRTX)*. Para obtener instrucciones para la instalación del firmware del CMC en el CMC en espera, consulte Actualización de firmware.

Modo a prueba de fallos de CMC

El gabinete PowerEdge VRTX activa el modo de prueba de fallas para proteger los módulos de E/S y los servidores de posibles fallas. Este modo se activa cuando no hay ningún CMC controlando el chasis. Durante el periodo de protección contra fallas del CMC o durante la pérdida de administración de un CMC:

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

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

- Extracción del CMC: la administración del chasis se reanuda después de que se reemplaza el CMC o se ejecuta una protección contra fallas al CMC en espera.
- Extracción del cable de red del CMC o pérdida de la conexión de red: la administración del chasis se reanuda después de que el chasis cede el control al CMC en espera después de una falla. La protección contra fallas de la red solo está activada en el modo de CMC redundante.
- Restablecimiento del CMC: la administración del chasis se reanuda después de que se reinicia el CMC o el chasis cede el control al CMC en espera después de una falla.

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

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

Proceso de elección del CMC activo

No hay ninguna diferencia entre las dos ranuras del CMC; es decir, la ranura no indica la prioridad. En lugar de eso, el CMC que se instala o se inicia primero asume la función del CMC activo. Si se aplica corriente alterna con dos CMC instalados, el CMC instalado en la ranura 1 del chasis del CMC generalmente se convierte en el CMC activo. El CMC activo se indica con el LED azul.

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

Obtención del estado de condición del CMC redundante

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

Configuración del panel frontal

Puede configurar los siguientes atributos:

- Botón de encendido
- LCD
- Unidad de DVD

Configuración del botón de encendido

Para configurar el botón de encendido del chasis:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Panel frontal** → **Configuración**.
2. En la página **Configuración del panel frontal**, en la sección **Configuración del botón de encendido**, seleccione la opción **Desactivar botón de encendido del chasis** y, a continuación, haga clic en **Aplicar**.

   Se desactiva el botón de encendido del chasis.

Configuración del LCD

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Panel anterior → Configuración**.
2. En la página **Configuración**, vaya a la sección **Configuración de LCD** y realice lo siguiente:
   - Seleccione la opción **Bloquear LCD de panel de control** para desactivar cualquier configuración que se pueda realizar con la interfaz del LCD.
   - Seleccione el idioma en el menú desplegable **Idioma de LCD**.
   - En el menú desplegable **Orientación de LCD**, seleccione el modo requerido: **modo de torre** o **modo de bastidor**.

   NOTA: Cuando configura el chasis mediante el asistente del LCD, si selecciona la opción **Aplicar automáticamente la configuración a los servidores recientemente insertados**, no puede desactivar la función **Aplicar automáticamente la configuración a los servidores recientemente insertados** con una licencia básica. Si no desea que la función surta efecto, ignore el mensaje que aparece en el LCD, que desaparecerá de forma automática; o bien, presione el botón **No aceptar** en el LCD y, a continuación, presione el botón central.
3. Haga clic en **Apply (Aplicar)**.

Acceso a un servidor mediante KVM

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

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

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

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

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

Asignación del servidor a KVM mediante la interfaz del LCD

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

Asignación de un servidor a una unidad de DVD

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

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Panel frontal → Configuración**.
2. En la página **Configuración del panel anterior**, dentro de la sección **Configuración de la unidad de DVD**:

En el menú desplegable **DVD asignado**, seleccione uno de los servidores. Seleccione los servidores para los cuales se requiere acceso a la unidad de DVD del chasis.

3. Haga clic en **Aplicar**.

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

3

Inicio de sesión en el CMC

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

Acceso a la interfaz web del CMC

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

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

Para acceder a la interfaz web del CMC:

1. Abra un explorador web compatible en el sistema.
   Para obtener información actualizada sobre los exploradores web admitidos, consulte *Dell Systems Software Support Matrix (Matriz de compatibilidad de software de los sistemas Dell)* que se encuentra en **dell.com/support/manuals**.
2. En el campo **Dirección**, escriba la siguiente dirección URL y presione <Intro>:
   - Para obtener acceso al CMC mediante la dirección IPv4: `https://<CMC IP address>`
     Si el número de puerto HTTPS predeterminado (puerto 443) se ha modificado, escriba: `https://<CMC IP address>:<port number>`
   - Para obtener acceso al CMC mediante la dirección IPv6: `https://[<CMC IP address>]`
     Si se cambió el número de puerto HTTPS predeterminado (puerto 443), escriba: `https://[<CMC IP address>]:<port number>`, donde <*CMC IP address*> es la dirección IP para CMC y <*port number*> es el número de puerto HTTPS.

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

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

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

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

NOTA:

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

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

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

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

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

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

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

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

Inicio de sesión en el CMC mediante una tarjeta inteligente

Para usar esta función, debe tener una licencia Enterprise. Es posible iniciar sesión en el CMC mediante una tarjeta inteligente. Las tarjetas inteligentes proporcionan autenticación de dos factores (TFA) que proporcionan dos capas de seguridad.

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

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

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

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

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

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

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

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

   NOTA: Si ha cambiado el número del puerto HTTPS predeterminado (puerto 80), ingrese a la página web del CMC mediante `<cmcname.domain-name>:<port number>`, donde nombredecmc es el nombre de host del CMC, *domain-name* es el nombre del dominio y *port number* es el número del puerto HTTPS.
2. Inserte la tarjeta inteligente y haga clic en **Iniciar sesión**.

   Se muestra el cuadro de diálogo PIN.
3. Introduzca el PIN y haga clic en **Enviar**.

   NOTA: Si el usuario de tarjeta inteligente está presente en Active Directory, no se requiere una contraseña de Active Directory. De otro modo, debe iniciar sesión mediante un nombre de usuario y una contraseña adecuados.

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

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

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

NOTA: No se puede utilizar la dirección IP para obtener acceso al inicio de sesión único. Kerberos valida las credenciales en función del nombre de dominio completo (FQDN).

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

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

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

1. Inicie sesión en el sistema cliente utilizando la cuenta de red.
2. Obtenga acceso a la interfaz web del CMC mediante: `https://<cmcname.domain-name>`.

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

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

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

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

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

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

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

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

   Ahora está conectado al CMC.

Acceso al CMC mediante RACADM

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

La interfaz RACADM se clasifica de la siguiente manera:

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

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

Es posible usar los comandos de RACADM remotos en secuencias para configurar varios CMC. No es posible ejecutar las secuencias directamente en el interfaz web del CMC, porque el CMC no lo admite.

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

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

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

Es posible iniciar sesión en el CMC a través de SSH sin introducir ninguna contraseña. También se puede enviar un único comando RACADM como un argumento de línea de comandos a la aplicación SSH. Las

opciones de línea de comandos presentan un comportamiento similar a las de RACADM remoto, ya que la sesión termina una vez completado el comando.

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

Por ejemplo:

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

Cuando se inicia sesión usando la cuenta de servicio, si la frase de contraseña se configuró en el momento de crear el par de clave pública o privada, es posible que el sistema solicite la introducción de esa frase de contraseña nuevamente. Si la frase de contraseña se utiliza con las claves, los sistemas cliente que ejecutan Windows y Linux proporcionan métodos para automatizar el método. En los sistemas cliente que ejecutan Windows, se puede usar la aplicación Pageant. Esta aplicación se ejecuta en segundo plano y hace que la introducción de la contraseña sea transparente. Para los sistemas cliente que ejecutan Linux, se puede usar el agente ssh. Para configurar y utilizar cualquiera de estas aplicaciones, consulte la documentación del producto correspondiente.

Varias sesiones en el CMC

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

Tabla 5. Varias sesiones en el CMC

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

Cambio de la contraseña de inicio de sesión predeterminada

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

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

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

un solo mensaje de advertencia para cada sesión. Para RACADM remoto, se muestra el mensaje de advertencia para cada comando.

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

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

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

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

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

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

   - 0-9
   - A-Z
   - a-z
   - Caracteres especiales: +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, I, \
3. En el campo **Confirmar contraseña**, escriba nuevamente la contraseña.
4. Haga clic en **Continuar**. Se configura la contraseña nueva y queda conectado al CMC.

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

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

Cambio de la contraseña de inicio de sesión predeterminada mediante RACADM

Para cambiar la contraseña, ejecute el siguiente comando RACADM:

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

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

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

Activación o desactivación del mensaje de advertencia de contraseña predeterminada

Es posible activar o desactivar la visualización del mensaje de advertencia de contraseña predeterminada. Para hacerlo, debe tener privilegio de **Configurar usuarios**.

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

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

1. Vaya a **Controladora del chasis → Autenticación de usuarios → Usuarios locales**.

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

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

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

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

4

Actualización de firmware

Es posible actualizar el firmware para:

- CMC: activo y en espera
- Infraestructura del chasis
- Módulo de E/S
- iDRAC
- PERC
- Dispositivo expansor y disco duro

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

- iDRAC
- BIOS
- Lifecycle Controller
- Diagnósticos de 32 bits
- Driver Pack del sistema operativo
- Controladoras de interfaz de red
- Controladoras RAID

Descarga de firmware del CMC

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

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

1. Firmware de los componentes de blade
2. Firmware del CMC
3. Firmware de infraestructura del chasis
4. Frmware de PERC 8 compartido
5. Firmware del plano posterior de almacenamiento
6. Firmware de la unidad de disco duro

Para obtener más información sobre la secuencia de actualización para el chasis VRTX, consulte *CMC Firmware 2.0 Release Notes* (Notas de la versión 2.0 del firmware del CMC 2.0) en el sitio de asistencia.

Visualización de versiones de firmware actualmente instaladas

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

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

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

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

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

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

Visualización de versiones de firmware actualmente instaladas mediante RACADM

Para ver la información de IP para iDRAC y CMC y el servicio de CMC o la etiqueta de propiedad mediante RACADM, ejecute el subcomando `racadm getsysinfo`. Para obtener más información acerca de otros comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX).

Actualización de firmware del CMC

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

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

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

tiempo de transferencia de archivos de firmware sea de hasta 30 minutos. Para configurar el valor de Tiempo de espera en inactividad, consulte Configuración de servicios.

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

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

NOTA:

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

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

Cuando se haya actualizado el CMC en espera, intercambie las funciones del CMC de modo que el CMC recientemente actualizado pase a ser el CMC activo y el CMC con el firmware anterior pase al modo en espera. Para obtener información acerca de cómo intercambiar las funciones, consulte la sección del comando `cmcchangeover` en *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX). La ejecución de este comando ayuda a verificar que la actualización se haya realizado satisfactoriamente y que el firmware nuevo esté funcionando adecuadamente, antes de actualizar el firmware en el segundo CMC. Cuando los dos CMC estén actualizados, es posible usar el comando `cmcchangeover` para restablecer los CMC a sus funciones anteriores. La revisión del firmware del CMC actualiza dos veces el CMC principal y el CMC redundante sin ejecutar el comando `cmcchangeover`.

Para evitar la desconexión de otros usuarios durante el restablecimiento, informe sobre este proceso a los usuarios autorizados con posibilidades de conectarse al CMC y compruebe si existen sesiones activas en la página **Sesiones**. Para abrir la página **Sesiones**, haga clic en **Descripción general del chasis** en el panel izquierdo, haga clic en **Red** y haga clic en **Sesiones**.

Cuando se trasfieran archivos al CMC y desde este, el icono de transferencia de archivos gira durante la transferencia. Si el icono no tiene animación, asegúrese de que el explorador esté configurado para permitir animaciones. Para obtener más información acerca de cómo permitir animaciones en el explorador, consulte Permitir animaciones en Internet Explorer.

Imagen firmada del firmware del CMC

Para VRTX CMC 2.0 y versiones posteriores, el firmware incluye una firma. El firmware del CMC verifica la firma para garantizar la autenticidad del firmware cargado. El proceso de actualización del firmware es

exitoso sólo si la imagen del firmware se autentica mediante el CMC para asegurarse de que sea una imagen válida del proveedor de servicios y de que no se ha alterado la misma. El proceso de actualización del firmware se detiene si el CMC no puede verificar la firma de la imagen del firmware cargado. Se registra un suceso de advertencia en el registro y se muestra el mensaje de error correspondiente.

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

Actualización de firmware del CMC mediante la interfaz web

NOTA: Antes de actualizar el firmware del CMC, asegúrese de encender el chasis, pero apague todos los servidores en el chasis.

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

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

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

Instrucciones adicionales:

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

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

Actualización de firmware del CMC mediante RACADM

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

Actualización del firmware de infraestructura del chasis

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

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

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

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

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

Instrucciones adicionales que hay que seguir:

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

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

Actualización del firmware de la infraestructura del chasis mediante RACADM

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

Actualización de firmware del iDRAC del servidor

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

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

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

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

Actualización de firmware del iDRAC del servidor mediante la interfaz web

Para actualizar el firmware del iDRAC en el servidor:

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

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

   NOTA:

   También es posible actualizar el firmware del iDRAC del servidor en **Descripción general del chasis → Descripción general del servidor → Actualizar**. Para obtener más información, consulte Updating Server Component Firmware (Actualización del firmware de los componentes del servidor).
2. Para actualizar el firmware del iDRAC7 o del iDRAC8, en la sección **Firmware del iDRAC7** o **Firmware del iDRAC8** respectivamente, haga clic en el vínculo **Actualizar** correspondiente al servidor cuyo firmware desee actualizar.

   Aparecerá la página **Actualización de los componentes del servidor**. Para continuar, consulte Updating Server Component Firmware (Actualización del firmware de los componentes del servidor).
3. En el campo **Imagen del firmware**, introduzca la ruta de acceso del archivo de imagen del firmware en la estación de administración o en la red compartida, o haga clic en **Examinar** para dirigirse a la ubicación del archivo. El nombre predeterminado de la imagen del firmware del iDRAC es **firmimg.imc**.
4. Haga clic en **Iniciar actualización del firmware** y, a continuación, en **Sí**.

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

NOTA: Instrucciones adicionales que hay que seguir:

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

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

Actualización de firmware de los componentes del servidor

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

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

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

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

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

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

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

NOTA: Tenga en cuenta lo siguiente:

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

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

  – BIOS
  – Lifecycle Controller
  – iDRAC

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

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

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

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

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

Si el servidor no admite el servicio Lifecycle Controller, la sección **Inventario de firmware de componentes y dispositivos** muestra **No admitido**. Para los servidores de última generación, instale el firmware de Lifecycle Controller y actualice el firmware del iDRAC para activar el servicio Lifecycle Controller en el servidor. Para los servidores de generaciones anteriores, es posible que esta actualización no pueda ejecutarse.

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

Es posible también instalar el firmware de Lifecycle Controller con un paquete de instalación adecuado ejecutado en el sistema operativo del servidor. Para obtener más información, consulte *Dell Lifecycle Controller User's Guide (Guía del usuario de Dell Lifecycle Controller)*.

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

`Lifecycle Controller may not be enabled.`

Secuencia de actualización de componentes del servidor

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

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

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

Activación de Lifecycle Controller

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

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

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

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

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

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

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

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

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

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

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

   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione el tipo de método de actualización necesario:
   - **Actualizar desde archivo**
   - **Actualizar desde recurso compartido de red**

Filtrado de componentes para actualizaciones de firmware

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

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

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

Estos filtros le permiten:

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

  NOTA: La función de filtro automático es importante al utilizar Dell Update Packages (DUP). La actualización de un paquete DUP se puede basar en el tipo o el modelo de un componente o dispositivo. El comportamiento de los filtros automáticos está diseñado para minimizar las decisiones de selección que se toman después una selección inicial.

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

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

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

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

Para filtrar los dispositivos:

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

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

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

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

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

Filtrado de componentes para actualizaciones de firmware mediante RACADM

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

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

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

Visualización del inventario de firmware

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

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

Visualización del inventario de firmware mediante la interfaz web del CMC

Para ver el inventario de firmware:

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

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

     1. Para los servidores del iDRAC, en la consola de inicio, para acceder a **Configuración del sistema**, presione <F2>.
     2. En la página **Menú principal de la configuración del sistema**, haga clic en **Configuración del iDRAC → Recopilar inventario del sistema al reinicio**, seleccione **Activado**, regrese a la página **Menú principal de la configuración del sistema** y haga clic en **Finalizar** para guardar la configuración.
   - Se encuentran disponibles las opciones para las diversas operaciones de Lifecycle Controller como Actualizar, Revertir, Reinstalar y Eliminación de trabajos. Solamente se puede realizar un tipo de operación a la vez. Los componentes y los dispositivos no admitidos pueden formar parte del inventario, pero no permiten las operaciones de Lifecycle Controller.

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

Tabla 6. Información sobre componentes y dispositivos

Campo	Descripción
Slot	Muestra la ranura que ocupa el servidor en el chasis. Los números de las ranuras son identificaciones secuenciales de 1 a 4 (para las 4 ranuras disponibles en el chasis), que ayudan a identificar la ubicación del servidor en el chasis. Cuando hay menos de 4 servidores que ocupan ranuras, solamente se muestran las ranuras ocupadas por servidores.
Name	Muestra el nombre del servidor en cada ranura.
Model	Muestra el modelo del servidor.
Componente/ Dispositivo	Muestra una descripción del componente o del dispositivo en el servidor. Si el ancho de la columna es demasiado estrecho, la herramienta pasar el mouse permite ver la descripción.
Versión actual	Muestra la versión actual del componente o del dispositivo en el servidor.
Versión de reversión	Muestra la versión de reversión del componente o del dispositivo en el servidor.
Estado del trabajo	Muestra el estado del trabajo de cualquier operación que se ha programado en el servidor. El estado del trabajo se actualiza constantemente de forma dinámica. Si se detecta la finalización de un trabajo, las versiones de firmware de los componentes y los dispositivos en ese servidor se actualizan automáticamente en caso de que se haya realizado un cambio de versión de firmware en alguno de los componentes o los dispositivos. También se expone un icono de información junto al estado actual, que proporciona información adicional sobre el estado del trabajo actual. Al hacer clic en el icono o mover el cursor sobre él, se puede ver esa información.
Actualizar	Haga clic en seleccionar el componente o dispositivo para la actualización de firmware del servidor.

Visualización del inventario de firmware mediante RACADM

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

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

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

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

Para guardar el informe de inventario del chasis:

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

   Aparecerá la página **Actualización de los componentes del servidor**.
2. Haga clic en **Guardar informe de inventario**.

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

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

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

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

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

   Se mostrará la sección **Editar recurso compartido de red**.
2. En la sección **Configuración de recurso compartido de red**, configure los siguientes valores según sea necesario:
   - Protocolo
   - Dirección IP o nombre del host
   - Nombre del recurso compartido
   - Carpeta de actualización
   - Nombre de archivo (opcional)

     NOTA: **Nombre de archivo** es opcional solamente cuando el nombre de archivo de catálogo predeterminado es *catalog.xml*. Si el nombre de archivo de catálogo se cambia, se debe introducir el nuevo nombre en este campo.
   - Carpeta de perfil
   - Domain Name
   - Nombre de usuario
   - Contraseña

   Para obtener más información, consulte *CMC Online Help (Ayuda en línea para el CMC)*.
3. Haga clic en **Probar directorio** para verificar si se permite lectura y escritura en los directorios.
4. Haga clic en **Probar conexión de red** para verificar si se puede acceder a la ubicación del recurso compartido de red.
5. Haga clic en **Aplicar** para aplicar los cambios en las propiedades del recurso compartido de red.

   NOTA:

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

Operaciones de Lifecycle Controller

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

Es posible realizar operaciones de Lifecycle Controller tales como:

- Reinstalar

- Rollback
- Actualizar
- Eliminar trabajos

Solamente se puede realizar un tipo de operación a la vez. Los componentes y los dispositivos no admitidos pueden formar parte del inventario, pero no permiten las operaciones de Lifecycle Controller.

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

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

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

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

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

Reinstalación del firmware de los componentes del servidor

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

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

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

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

Reversión del firmware de los componentes del servidor

Es posible instalar la imagen de firmware del firmware previamente instalado para componentes o dispositivos seleccionados en uno o varios servidores. La imagen de firmware está disponible en Lifecycle Controller para una operación de reversión. La disponibilidad está sujeta a la lógica de compatibilidad con la versión de Lifecycle Controller. También se presupone que Lifecycle Controller ha facilitado la actualización anterior.

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

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

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

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

Actualización de firmware de los componentes del servidor

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

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

Se recomienda borrar la fila de trabajo en espera antes de inicializar una actualización de firmware para los componentes del servidor. Una lista de todos los trabajos en los servidores está disponible en la página **Lifecycle Controller Jobs**. Esta página permite eliminar uno o varios trabajos o depurar todos los trabajos en el servidor.

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

Si el tamaño de la imagen en el archivo de actualización es mayor, el estado del trabajo indica que se ha producido una falla en la descarga. Si se intentan varias actualizaciones de componentes a la vez en un servidor, el tamaño combinado de todos los archivos de actualización de firmware puede superar los 48 MB. En ese caso, una de las actualizaciones en el componente falla, ya que el archivo de actualización se trunca. Una estrategia recomendada para actualizar varios componentes en un servidor es primero actualizar juntos los componentes de Diagnósticos de 32 bits y Lifecycle Controller. Estas actualizaciones no requieren reiniciar el servidor y se completan relativamente rápido. Los demás componentes pueden actualizarse juntos después.

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

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

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

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

   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde archivo**. Para obtener más información, consulte la sección Elección del tipo de actualización del firmware de los componentes del servidor mediante la interfaz web del CMC.
3. En la sección **Filtro para actualizar componentes y dispositivos**, filtre el componente o el dispositivo (opcional). Para obtener más información, consulte Filtrado de componentes para actualizaciones de firmware mediante la interfaz web del CMC.
4. En la columna **Actualizar**, seleccione las casillas para el componente o el dispositivo en el que desea actualizar el firmware a la siguiente versión. Utilice el acceso directo con la tecla CRTL para seleccionar un tipo de componente o dispositivo que se actualice en todos los servidores aplicables. Si mantiene presionada la tecla CRTL, se resaltan todos los componentes en amarillo. Mientras mantiene presionada la tecla CRTL, active la casilla asociada en la columna **Actualizar** para seleccionar el componente o el dispositivo necesario.

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

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

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

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

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

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

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

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

Este método proporciona una forma rápida y fácil de crear un repositorio personalizado para los sistemas conectados que posea mediante Dell Repository Manager y el archivo de inventario del chasis exportado por medio de la interfaz web del CMC. DRM le permite crear un repositorio totalmente personalizado que solamente incluye los paquetes de actualización para la configuración específica del sistema. También puede crear repositorios que solamente contengan actualizaciones para dispositivos obsoletos, o bien, un repositorio básico que contenga actualizaciones para todos los dispositivos. También puede crear conjuntos de paquetes de actualización para Linux o Windows según el modo de actualización necesario. DRM le permite guardar el repositorio en un recurso compartido de CIFS o NFS. La interfaz web del CMC permite configurar los detalles de la ubicación y las credenciales para el recurso compartido. Mediante la interfaz web del CMC, puede realizar a continuación la actualización de los componentes del servidor para un solo servidor o múltiples servidores.

Requisitos previos para utilizar el modo de actualización de recursos compartidos de red

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

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

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

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

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

   Aparecerá la página **Actualización de los componentes del servidor**.
2. En la sección **Seleccionar tipo de actualización**, seleccione **Actualizar desde recurso compartido de red**. Para obtener más información, consulte la sección Elección de tipo de actualización del firmware de los componentes del servidor.
3. Si el recurso compartido de red no se encuentra conectado, configure el recurso compartido de red para el chasis. Para configurar o editar los detalles del recurso compartido de red, en la tabla Propiedades del recurso compartido de red, haga clic en **Editar**. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web del CMC.
4. Haga clic en **Guardar informe de inventario** para exportar el archivo de inventario del chasis que contiene los detalles de los componentes y el firmware.

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

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

   NOTA: Haga clic en **Contraer** en una ranura para contraer los detalles del firmware de componentes y dispositivos de la ranura específica. De forma alternativa, para ver todos los detalles de nuevo, haga clic en **Expandir**.
6. En la sección **Inventario de firmware de componentes y dispositivos**, seleccione la casilla junto a **Seleccionar/Deseleccionar todo** para seleccionar todos los servidores compatibles. De forma alternativa, seleccione la casilla junto al servidor en el que desea actualizar el firmware de los componentes. No se pueden seleccionar componentes individuales para el servidor.
7. Seleccione una de las siguientes opciones para especificar si es necesario reiniciar el sistema después de programar las actualizaciones:
   - Reiniciar ahora: Se programan las actualizaciones, se reinicia el servidor y, a continuación, se aplican inmediatamente las actualizaciones a los componentes del servidor.
   - En el siguiente reinicio: Las actualizaciones se programan, pero solo se aplican después del siguiente reinicio del servidor.
8. Haga clic en **Actualizar** para programar las actualizaciones de firmware en los componentes disponibles de los servidores seleccionados.

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

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

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

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

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

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

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

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

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

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

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

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Actualizar**.
2. En la página **Actualización de componentes de almacenamiento**, haga clic en **Examinar**.

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

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

   El DUP está cargado en el CMC. La sección **Actualización de los componentes de almacenamiento** muestra solo los componentes que son compatibles con el archivo de DUP descargado. Aparecen la versión actual, la versión más reciente disponible y la casilla de verificación **Actualizar** para los componentes.
5. Seleccione las casillas de verificación **Actualizar** que corresponda para los componentes necesarios.
6. Haga clic en **Update (Actualizar)**.

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

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

NOTA: Los servidores deben apagarse antes de actualizar el firmware.

Recuperación de firmware del iDRAC mediante el CMC

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

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

5

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

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

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

Visualización de los resúmenes de los componentes y el chasis

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



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

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

Gráficos del chasis

El chasis se representa mediante las vistas anterior y posterior (las imágenes superiores e inferiores respectivamente). Los servidores, DVD, HDD, KVM y LCD se muestran en la vista anterior y los componentes restantes se muestran en la vista posterior. La selección de los componentes está indicada en azul y se controla al hacer clic en la imagen del componente requerido. Cuando un componente está presente en el chasis, se muestra un icono del tipo de componente en los gráficos en la posición (ranura), en donde se ha instalado el componente. Las posiciones vacías se muestran con un fondo gris. El icono del componente indica visualmente su estado. Otros componentes muestran iconos que representan visualmente el componente físico. Al pasar el cursor sobre un componente, aparece información sobre herramientas con información adicional acerca del componente.

Tabla 7. Estados del icono del servidor

Icono	Descripción
	Un servidor está presente, encendido, y opera normalmente.
	Un servidor está presente, pero apagado.
	Un servidor está presente pero informa un error no crítico.
	Un servidor está presente pero informa un error crítico.

Icono	Descripción
	Un servidor no está presente.

Información del componente seleccionado

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

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

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

Component	Propiedades de condición y rendimiento	Propiedades	Vínculos rápidos
Conjunto del LCD	• Condición de LCD • Condición del chasis	• Botón de encendido del chasis • Bloquear panel de control de LCD • Idioma de LCD • Orientación de LCD	Configuración del panel frontal
CMC activos y en espera	• Modo de redundancia • Dirección MAC • IPv4 • IPv6	• Firmware • Firmware en espera • Última actualización • Hardware	• Estado del CMC • Networking (Sistema de red) • Actualización del firmware
Todos los servidores y servidores individuales	• Estado de la alimentación • Consumo de alimentación • Health • Energía asignada • Temperatura	• Name • Model • Etiqueta de servicio • Nombre del host • iDRAC • CPLD • BIOS • SO • Información de la CPU	• Estado del servidor • Iniciar la consola remota • Iniciar la interfaz gráfica de usuario del iDRAC • Apagar el servidor • Apagado ordenado • Recurso compartido de archivos remotos • Implementar red de iDRAC • Actualización de componentes del servidor

		• Memoria total del sistema	**NOTA:** Los vínculos rápidos Apagar el servidor y Apagado ordenado se muestran solamente si el estado de energía del servidor es Encendido. Si el estado de energía del servidor es Apagado, se muestra el vínculo rápido Encender servidor.
Ranura de KVM	Health	• KVM asignado • Ranura 1: USB/video del panel frontal activado • Ranura 2: USB/video del panel frontal activado • Ranura 3: USB/video del panel frontal activado • Ranura 4: USB/video del panel frontal activado	Configuración del panel frontal
Ranura de DVD	• Health • Estado de la alimentación	• DVD asignado • Ranura 1: DVD activado • Ranura 2: DVD activado • Ranura 3: DVD activado • Ranura 4: DVD activado	Configuración del panel frontal
Ranura de disco	• Health • Status	• Model • Serial Number • Estado de la alimentación • Firmware Version • Size • Tipo	• Estado del disco físico • Configuración del disco físico • Ver controladora para este disco físico • Ver discos virtuales para este disco físico
Unidades de suministro de energía	Estado de la alimentación	Capacity	• Estado del suministro de energía • Consumo de alimentación • Presupuesto del sistema
Dispositivos PCIe	• Instalada • Asignado	• Model • Asignación de ranura del servidor • Id. de vendedor • Id. de dispositivo	• Estado de PCIe • Configuración de PCIe

		• Slot Type • Alimentación asignada • Red Fabric • Estado de la alimentación	
Ventiladores	• Speed • PWM (% del máximo) • Desplazamiento del ventilador	• Umbral de aviso • Umbral crítico	• Estado de los ventiladores • Configuración del ventilador
Ventilación	• Speed • PWM (% del máximo) • Modo de enfriamiento mejorado	• Umbral de aviso • Umbral crítico	• Estado de los ventiladores • Configuración del ventilador
Ranura SPERC	• Instalada • Asignado	• Model • Asignación de ranura del servidor • Id. de vendedor • Id. de dispositivo • Slot Type • Alimentación asignada • Red Fabric • Estado de la alimentación	• Estado de la controladora • Configuración de la controladora
Ranura del módulo de E/S	• Estado de la alimentación • Role	• Model • Etiqueta de servicio	Estado del módulo de E/S Iniciar interfaz gráfica de usuario del módulo de E/S

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

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

1. En el panel izquierdo, bajo el nodo de árbol **Descripción general de servidores**, todos los servidores (SLOT-01 a SLOT-04) aparecen en la lista de servidores. Si un servidor no está presente en la ranura, la imagen correspondiente en el gráfico aparecerá atenuada. Cuando los servidores de altura completa están presentes en la ranura 1 y en la ranura 3, la ranura 3 mostrará el nombre de ranura como **Extensión de 1**.
2. Pase el cursor sobre el nombre o el número de ranura de un servidor. Aparece información sobre herramientas con el nombre de modelo del servidor y la etiqueta de servicio (si está disponible).

Visualización del resumen del chasis

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

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

Visualización de información y estado de la controladora del chasis

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

Aparecerá la página **Estado de la controladora del chasis**. Para obtener más información, consulte *Online Help* (Ayuda en línea).

Visualización de información y estado de condición de todos los servidores

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

- Haga clic en **Descripción general del chasis**. La página **Condición del chasis** mostrará una descripción gráfica de todos los servidores instalados en el chasis. El estado de condición de los servidores se indica con la superposición del subgráfico de los servidores. Para obtener más información, consulte la *ayuda en línea*.
- Haga clic en **Descripción general del chasis → Descripción general del servidor**. La página **Estado del servidor** ofrece una descripción general de los servidores del chasis. Para obtener más información, consulte la *ayuda en línea*.

Visualización de información y estado de condición de un servidor individual

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

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

   La página **Condición del chasis** mostrará una descripción gráfica de todos los servidores instalados en el chasis. El estado de la condición de cada servidor se indica con la superposición del gráfico secundario del servidor. Mueva el cursor sobre el gráfico secundario de un servidor individual. La sugerencia de texto o la explicación en pantalla correspondiente brinda información adicional sobre ese servidor. Haga clic en el gráfico secundario del servidor para ver la información del módulo de E/S a la derecha. Para obtener más información, consulte la *Ayuda en línea*.
2. Vaya a **Descripción general del chasis** y **expanda Descripción general del servidor** en el panel izquierdo. Todos los servidores (1 a 4) aparecerán en la lista expandida. Haga clic en el servidor (la ranura) que desea ver.

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

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

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

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

1. Haga clic en **Descripción general del chasis**.
   Se muestra la página **Condición del chasis**. Los gráficos en el panel izquierdo muestran la vista posterior, anterior y lateral del chasis y contiene el estado del módulo de E/S. El estado del módulo de E/S está indicado por la superposición del subgráfico del módulo de E/S. Mueva el cursor por el subgráfico del módulo de E/S individual. La sugerencia de texto proporciona información adicional acerca del módulo de E/S. Haga clic en el subgráfico del módulo de E/S para ver la información correspondiente en el panel derecho.
2. Vaya a **Descripción general del chasis → Descripción general del módulo de E/S**.
   La página **Estado del módulo de E/S** proporciona una descripción general de los módulos de E/S asociados con el chasis. Para obtener más información, consulte *Online Help (Ayuda en línea)*.

Visualización de información y estado de condición de los ventiladores

CMC controla la velocidad del ventilador del chasis al aumentar o disminuir la velocidad del ventilador según los sucesos del sistema. Es posible ejecutar el ventilador en tres modos: Bajo, Medio y Alto. Para obtener más información sobre cómo configurar un ventilador, consulte la *ayuda en línea*.

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

```
racadm fanoffset [-s <apagado|bajo|medio|alto>]
```

NOTA: El CMC supervisa los sensores de temperatura en el chasis y automáticamente ajusta la velocidad del ventilador según sea necesario. Sin embargo, es posible realizar una sustitución para mantener una velocidad mínima del ventilador mediante el comando racadm fanoffset. Cuando se realiza la sustitución con este comando, el CMC siempre ejecuta el ventilador en la velocidad seleccionada, aun cuando el chasis no requiere que los ventiladores se ejecuten a esa velocidad.

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

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 deja de funcionar.
- Se desmonta un ventilador del chasis.

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

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

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

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

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

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

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

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

   ```
   Fan <number> RPM is less than the lower critical threshold. (La
   velocidad en RPM del ventilador <número> está por debajo del umbral
   crítico inferior).
   ```

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

Configuración de ventiladores

Desplazamiento del ventilador: es una función que ofrece un mayor enfriamiento para el almacenamiento y las regiones de PCIe del chasis. Esta función permite aumentar la distribución de flujo de aire en HDD, controladoras Shared PERC y ranuras de tarjeta PCIe. Un ejemplo de uso de la función Desplazamiento del ventilador es cuando se utilizan tarjetas PCIe personalizadas o de alta potencia que requieren un mayor enfriamiento de lo normal. Esta función incluye las opciones Apagado, Bajo, Medio y Alto. Esta configuración corresponde a un desplazamiento de velocidad de ventilador (aumento) del 20 %, 50 % y 100 % de la velocidad máxima respectivamente. También hay opciones de configuración de velocidades mínimas para cada opción, que son 35 % para Bajo, 65 % para Medio y 100 % para Alto.

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

Con cualquiera de las opciones de Desplazamiento del ventilador activadas, aumenta el consumo de alimentación. El sistema será un poco ruidoso con el desplazamiento Bajo, bastante ruidoso con el desplazamiento Medio y muy ruidoso con el desplazamiento Alto. Cuando la opción Desplazamiento del ventilador no está activada, las velocidades del ventilador se reducen a las velocidades predeterminadas que se requieren para el enfriamiento del sistema para la configuración del hardware instalado.

Para establecer la función de desplazamiento, vaya a **Descripción general del chasis → Ventiladores → Configuración.**En la página **Configuraciones avanzadas del ventilador**, en la tabla **Configuración de ventilador**, en el menú desplegable **Valor** correspondiente a **Compensación del ventilador**, seleccione una opción de manera correcta.

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

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

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

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

Modo de enfriamiento mejorado (ECM): es una función del CMC que permite una capacidad de enfriamiento mayor para los servidores instalados en el chasis PowerEdge VRTX. Algunos ejemplos de uso de ECM son la operación en entornos con temperaturas ambiente elevadas o el uso de servidores con CPU de alta potencia (≥120W) instalados. La capacidad de enfriamiento mejorado se logra al permitir que los cuatro módulos de ventilación del chasis se ejecuten a una velocidad más alta. Como consecuencia, el consumo de alimentación del sistema y el nivel de ruido pueden aumentar si ECM está activado.

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

De forma predeterminada, el ECM está apagado. Si el ECM está activado, los sopladores tienen la capacidad para distribuir aproximadamente un 20 % más de flujo de aire por tarjeta.

Para establecer el modo de ECM, vaya a **Descripción general del chasis → Ventiladores → Configuración.**En la página **Configuraciones avanzadas del ventilador**, en la tabla **Configuración de la ventilación**, en el menú desplegable **Valor** correspondiente para **Modo de enfriamiento mejorado**, seleccione una opción de manera correcta.

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

Visualización de las propiedades del panel frontal

Para ver las propiedades del panel frontal:

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

Visualización de información y estado de condición del KVM

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

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

Aparece la página **Condición del chasis**. El panel izquierdo muestra la vista frontal del chasis y contiene el estado de condición de un KVM. El estado de condición de un KVM se indica con la superposición del subgráfico del KVM. Mueva el puntero por el subgráfico de un KVM para que aparezca la sugerencia de texto o el consejo de pantalla correspondiente. La sugerencia de texto proporciona información adicional acerca del KVM. Haga clic en el subgráfico del KVM para ver la información del KVM en el panel derecho.

2. De manera alternativa, haga clic en **Descripción general del chasis** → **Panel anterior**.

   En la página **Estado**, en la sección **Propiedades de KVM**, se pueden ver el estado y las propiedades de un KVM asociado con el chasis. Para obtener más información, consulte la *ayuda en línea*.

Visualización de información y condición de la pantalla LCD

Para ver el estado de la condición de un LCD:

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

   Aparece la página **Condición del chasis**. El panel izquierdo muestra la vista frontal del chasis. El estado de la condición del LCD se indica mediante la superposición del subgráfico del LCD.

2. Mueva el cursor sobre el subgráfico de la pantalla LCD. La sugerencia de texto o la explicación en pantalla correspondiente brinda información adicional sobre la pantalla LCD.
3. Haga clic en el subgráfico del LCD para ver la información del LCD en el panel derecho. Para obtener más información, consulte la *ayuda en línea*.

   De forma alternativa, vaya a **Descripción general del chasis** → **Panel anterior** → **Propiedades** → **Estado**. En la página **Estado**, en **Propiedades de LCD**, se puede ver el estado del LCD disponible en el chasis. Para obtener más información, consulte la *ayuda en línea*.

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

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

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

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

NOTA: El valor de las sondas de temperatura no se puede editar. Cualquier cambio fuera del umbral genera una alerta que causa que la velocidad de los ventiladores varíe. Por ejemplo, cuando la sonda de temperatura ambiente del CMC supera el umbral, la velocidad de los ventiladores del chasis aumenta.

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

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

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

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

La sección inferior de los gráficos del chasis proporciona la vista izquierda del chasis. Mueva el cursor sobre el gráfico secundario del componente de almacenamiento. El cuadro de texto proporciona información adicional sobre el componente de almacenamiento. Haga clic en el gráfico secundario del componente de almacenamiento para ver la información relacionada en el panel de la derecha.

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

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

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

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

   - Ver los sucesos de almacenamiento registrados recientemente.

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

6

Configuración del CMC

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

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

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

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

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

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

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

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

Visualización y modificación de la configuración de red LAN del CMC

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

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

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

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

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

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

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

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

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

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

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

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

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

Activación de la interfaz de red del CMC

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

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

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

Para activar o 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 o desactivar el direccionamiento IPv6 del CMC, escriba:

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

NOTA: Tenga en cuenta lo siguiente:

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

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

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

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

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

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

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

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

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

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

Activación o desactivación de DHCP para las direcciones IP de DNS

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

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

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

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

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

Establecimiento de direcciones IP estáticas de DNS

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

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

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

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

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

Configuración de DNS (IPv4 e IPv6)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

donde:

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

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

donde:

<*speed*> es 10 o 100 (valor predeterminado).

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

La propiedad MTU permite establecer un límite para el paquete más grande que se puede transferir a través de la interfaz. Para definir la MTU, escriba:

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

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

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

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

Las funciones de bloqueo de direcciones IP y de bloqueo de usuarios en el CMC le permiten evitar problemas de seguridad provocados por intentos de ataques de contraseñas. Esta función le permite bloquear un rango de direcciones IP y de usuarios que pueden acceder al CMC. De manera predeterminada, la función de bloqueo de direcciones IP está activada en el CMC.

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

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

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

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

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

1. En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Red → Red**. Aparecerá la página **Configuración de la red**.
2. En la sección Configuración de IPv4, haga clic en **Opciones avanzadas**.

Aparecerá la página **Seguridad de inicio de sesión**.

De manera alternativa, para acceder a la página Seguridad de inicio de sesión, en el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en**Seguridad → Inicio de sesión**.

3. Para activar la función de verificación de rango de IP, en la sección **Rango de IP**, seleccione la opción **Rango de IP activado**.

   Se activarán los campos **Dirección de rango de IP** y **Máscara de rango de IP**.

4. En los campos **Dirección de rango de IP** y **Máscara de rango de IP**, escriba el rango de direcciones IP y de máscaras de rangos de IP para los que desea bloquear el acceso al CMC.

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

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

Configuración de los atributos de rango de IP con RACADM

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

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

El filtrado de IP compara la dirección IP de un inicio de sesión entrante con el rango de direcciones IP especificado. Un inicio de sesión desde la dirección IP entrante se permite solo si los siguientes valores son idénticos:

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

NOTA:

- Para activar la función de verificación de rango IP, use la siguiente propiedad en el grupo `cfgRacTuning`:

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

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

  `cfgRacTuneIpRangeMask`

Configuración de las propiedades de la etiqueta LAN virtual para CMC

La función de LAN virtual permite que varias VLAN coexistan en el mismo cable de red físico y segreguen el tráfico de red por motivos de seguridad o de administración de carga. Cuando se activa la función de VLAN, se asigna una etiqueta VLAN a cada paquete de red.

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

1. Active las capacidades de LAN virtual (VLAN) de la red de administración del chasis externo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1
   ```
2. Especifique la identificación de VLAN para la red de administración del chasis externo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
   ```
   Los valores válidos para <*VLAN id*> son 1 a 4000 y 4021 a 4094. El valor predeterminado es 1.

   Por ejemplo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID 1
   ```
3. A continuación, especifique la prioridad de VLAN para la red de administración del chasis externo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority <VLAN priority>
   ```
   Los valores válidos para *<VLAN priority>* son de 0 a 7. El valor predeterminado es 0.

   Por ejemplo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7
   ```
   También puede especificar la identificación y la prioridad de VLAN con un solo comando:
   ```
   racadm setniccfg -v <VLAN id> <VLAN priority>
   ```
   Por ejemplo:
   ```
   racadm setniccfg -v 1 7
   ```
4. Para eliminar la VLAN del CMC, desactive las capacidades de VLAN de la red de administración del chasis externo:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 0
   ```
   También puede eliminar la VLAN del CMC con el siguiente comando:
   ```
   racadm setniccfg -v
   ```

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

Para configurar la LAN virtual (VLAN) para el CMC mediante la interfaz web del CMC:

1. Desplácese a cualquiera de las siguientes páginas:
   - En el panel izquierdo, haga clic en **Descripción general del chasis** y luego en **Red** → **VLAN**.
   - En el panel izquierdo, haga clic en **Descripción general del chasis** → **Descripción general del servidor** y, a continuación, en**Red** → **VLAN**.

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

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

Configuración de servicios

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

- Consola serie del CMC: permita el acceso al CMC mediante la consola serie.
- Servidor web: permita el acceso a la interfaz web del CMC. La desactivación del servidor web también desactiva RACADM remoto.
- SSH: permita el acceso al CMC mediante la funcionalidad RACADM de firmware.
- Telnet: permita el acceso al CMC mediante la funcionalidad RACADM de firmware.
- RACADM: permita el acceso al CMC mediante la funcionalidad RACADM.
- SNMP: active el CMC para enviar capturas SNMP para los sucesos.
- Syslog remoto: permita el CMC para registrar sucesos en un servidor remoto. Para usar esta función, debe tener una licencia Enterprise.

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

Si se restablece Web Server, espere al menos un minuto para que los servicios vuelvan a estar disponibles. En general, Web Server se restablece como resultado de alguno de los siguientes sucesos:

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

NOTA: Para modificar los ajustes de los servicios, deberá tener privilegios de Administrador de configuración del chasis.

El syslog remoto es un destino de registro adicional para el CMC. Después de configurar el syslog remoto, cada nueva anotación de registro generada por CMC se reenviará a los destinos.

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

Configuración de los servicios mediante la interfaz web del CMC

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

1. En el panel de la izquierda, haga clic en **Descripción general del chasis** y, a continuación, en **Red** → **Servicios**. Aparece la página **Administración de servicios**.
2. Configure los servicios siguientes según sea necesario:
   - Serie CMC
   - Web Server
   - SSH

- Telnet
- RACADM remoto
- SNMP
- Syslog remoto

Para obtener información acerca de los campos, consulte la *ayuda en línea*.

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

Configuración de servicios mediante RACADM

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

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

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

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

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

Por ejemplo:

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

Configuración de la tarjeta de almacenamiento extendido del CMC

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

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

1. En el panel izquierdo, vaya a **Descripción general del chasis** y, a continuación, haga clic en **Controladora del chasis → Medios flash**.
2. En la página **Medios flash extraíbles**, en el menú desplegable, seleccione una de las siguientes opciones según corresponda:
   - **Reparar medios del controlador activo**
   - **Detener el uso de los medios flash para almacenar datos del chasis**

Para obtener más información sobre estas opciones, consulte *Online Help* (Ayuda en línea).

3. Haga clic en **Aplicar** para aplicar la opción seleccionada.

   Si dos CMC están presentes en el chasis, los dos CMC (activo y en estado de espera) deben contener medios flash. De lo contrario, la funcionalidad de almacenamiento extendido debe estar degradado a menos que los CMC activo y en estado de espera contengan medios flash.

Configuración de un grupo de chasis

El CMC permite controlar varios chasis desde un solo chasis principal. Cuando se activa un grupo de chasis, el CMC del chasis principal genera un gráfico sobre el estado del chasis principal y de los demás chasis del grupo. Para usar esta función, debe contar con una licencia Enterprise.

Las funciones del grupo de chasis son las siguientes:

- Muestra imágenes con la parte delantera y posterior de cada chasis; un conjunto para el chasis principal y un conjunto para cada miembro.
- Los problemas en la condición del chasis principal y de los miembros de un grupo se marcan en rojo o amarillo y con una X o el signo ! en el componente que muestra los síntomas. Los detalles se muestran debajo de la imagen del chasis al hacer clic en la imagen o en **Detalles**.
- Los vínculos de inicio rápido están disponibles para abrir las páginas web del servidor o del chasis miembro.
- Hay un servidor y un inventario de entradas/salidas disponibles para un grupo.
- Existe una opción seleccionable para sincronizar las propiedades del miembro nuevo con las propiedades del principal cuando el miembro nuevo se agrega al grupo.

Un grupo de chasis puede contener hasta ocho miembros. Además, un chasis principal o miembro solo puede participar en un grupo. No se puede unir un chasis, ya sea principal o miembro, a otro grupo si ya forma parte de un grupo. Es posible eliminar el chasis de un grupo y agregarlo más adelante a un grupo diferente.

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

1. Inicie sesión en el chasis principal con los privilegios de administrador de chasis.
2. Haga clic en **Configuración → Administración de grupos**.
3. En la página **Grupo de chasis**, en **Función**, seleccione **Principal**. Aparecerá un campo para agregar el nombre de grupo.
4. Introduzca el nombre de grupo en el campo **Nombre del grupo** y haga clic en **Aplicar**.

   NOTA: Los nombres de dominio siguen las mismas reglas.

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

Adición de miembros a un grupo de chasis

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

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

5. En el campo **Nombre de usuario** introduzca un nombre de usuario con privilegios de administrador para el chasis miembro.
6. Introduzca la contraseña correspondiente en el campo **Contraseña**.
7. De manera opcional, seleccione **Sincronizar el miembro nuevo con las propiedades del principal** para enviar las propiedades del chasis principal al nuevo.
8. Haga clic en **Aplicar**.
9. Para agregar un máximo de ocho miembros, complete las tareas en el paso 4 al 8. Los nombres de chasis de los miembros nuevos aparecen en el cuadro de diálogo **Miembros**.

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

Eliminación de un miembro del chasis principal

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

1. Inicie sesión en el chasis principal con los privilegios de administrador de chasis.
2. En el panel izquierdo, seleccione el chasis principal.
3. Haga clic en **Configuración → Administración de grupos**.
4. En la lista **Eliminar miembros**, seleccione el nombre de los miembros que desea eliminar y, a continuación, haga clic en **Aplicar**.

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

Forma de desmontar un grupo de chasis

Para extraer totalmente un grupo del chasis principal:

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

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

   Si un problema de red evita el contacto entre el chasis líder y el chasis miembro, este último puede no recibir el mensaje. En este caso, desactive el miembro del chasis miembro para completar el proceso de eliminación.

Desactivación de un miembro del chasis miembro

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

1. Inicie sesión en el chasis miembro con privilegios de administrador.
2. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Configuración** → **Administración de grupos**.
3. Seleccione **Ninguno** y, a continuación, haga clic en **Aplicar**.

Acceso a la página web de un chasis miembro o servidor

Es posible acceder a la página web del chasis miembro, la consola remota del servidor o la página web del servidor iDRAC desde la página del grupo de chasis principal. Si el dispositivo miembro tiene las mismas credenciales de inicio de sesión que el chasis principal, puede usar las mismas credenciales para acceder al dispositivo miembro.

NOTA: No se admiten el inicio de sesión único ni el inicio de sesión mediante tarjeta inteligente en la administración de varios chasis. Para acceder a los miembros por medio del inicio de sesión único desde el chasis principal se requiere un nombre de usuario o una contraseña común entre el líder y los miembros. El uso de un nombre de usuario o una contraseña común solamente funciona con usuarios de Active Directory, locales y de LDAP.

Para desplazarse a los dispositivos miembro:

1. Inicie sesión en el chasis principal.
2. Seleccione **Grupo: nombre** en el árbol.
3. Si el destino necesario es un CMC miembro, seleccione **Iniciar CMC** para el chasis necesario.

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

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

Propagación de las propiedades del chasis principal al chasis miembro

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

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

principal se propagan a los miembros del grupo solo cuando el administrador del chasis principal hace clic en **Propagar**.

5. En la sección **Propiedades de propagación**, seleccione las categorías de las propiedades de configuración del chasis principal a propagar a los chasis miembro.

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

6. Haga clic en **Save (Guardar)**.

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

Inventario del servidor para el grupo de MCM

Un grupo es un chasis principal que contiene entre 0 y 8 miembros. La página **Condición del grupo de chasis** muestra todos los chasis miembro y permite guardar el informe de inventario del servidor en un archivo mediante la capacidad estándar de descarga del explorador. El informe contiene datos sobre:

- Todos los servidores presentes actualmente en todos los chasis del grupo (incluido el principal).
- Las ranuras vacías y las ranuras de extensión (incluidos los módulos del servidor de altura total y de doble ancho).

Forma de guardar el informe de inventario del servidor

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

1. En el panel izquierdo, seleccione el **Grupo**.
2. En la página **Condición del grupo de chasis**, haga clic en **Guardar informe de inventario**. Aparecerá el cuadro de diálogo **Descarga de archivo** y le pedirá que abra o guarde el archivo.
3. Haga clic en **Guardar** y especifique la ruta de acceso y el nombre de archivo para el informe de inventario del módulo del servidor.

   NOTA: El grupo de chasis principal y el grupo de chasis de miembro, así como el módulo del servidor del chasis asociado, deben estar encendidos para poder obtener el informe de inventario del módulo más preciso.

Datos exportados

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

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

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

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

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

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

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

Tabla 8. Descripciones de los campos de inventario del módulo del servidor

Campo de datos	Ejemplo
Nombre del chasis	Chasis principal del centro de datos
Dirección IP del chasis	192.168.0.1
Ubicación de ranura	1
Nombre de ranura	RANURA-01
Nombre del host	Web Server corporativo **NOTA:** Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.
Sistema operativo	Windows Server 2008 **NOTA:** Requiere que haya un agente Server Administrator en ejecución en el servidor; de lo contrario, se mostrará en blanco.
Modelo	PowerEdgeM610
Etiqueta de servicio	1PB8VF1
Memoria total del sistema	4.0 GB **NOTA:** Requiere VRTX CMC 1.0 (o posterior) en el miembro; de lo contrario, se mostrará en blanco.
N.º de CPU	2 **NOTA:** Requiere VRTX CMC 1.0 (o posterior) en el miembro; de lo contrario, se mostrará en blanco.
Información de CPU	CPU Intel (R) Xeon (R) E5502 a 1.87 GHzn **NOTA:** Requiere VRTX CMC 1.0 (o posterior) en el miembro; de lo contrario, se mostrará en blanco.

Formato de datos

El informe de inventario se genera en un formato de archivo **.CSV**, de modo que se pueda importar en varias herramientas, por ejemplo, Microsoft Excel. El archivo **.CSV** del informe de inventario se puede importar en la plantilla al seleccionar **Datos** → **Desde texto** en MS Excel. Una vez que el informe de

inventario se haya importado en MS Excel y aparezca un mensaje para solicitar información adicional, seleccione Delimitado por comas para importar el archivo en MS Excel.

Inventario del grupo de chasis y versión de firmware

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

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

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

Visualización del inventario del grupo de chasis

Para ver el grupo de chasis mediante la interfaz web del CMC, en el panel izquierdo, seleccione **Grupo**. Haga clic en **Propiedades → Versión de firmware**. Aparecerá la página **Versión de firmware del grupo de chasis**, que muestra todos los chasis en el grupo.

Visualización del inventario del chasis seleccionado con la interfaz web

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

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

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

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

1. En el panel izquierdo, seleccione **Grupo**. Haga clic en **Propiedades → Versión de firmware**.
   La página **Versión de firmware del grupo de chasis** muestra todos los chasis en el grupo.
2. En la sección **Seleccionar un chasis**, seleccione el chasis miembro del que desea ver el inventario.
3. En la sección **Filtro de visualización de firmware**, seleccione **Componentes**.

4. En la lista **Componentes**, seleccione el componente requerido (BIOS, iDRAC, CPLD, USC, Diagnóstico, unidad de SO, dispositivos RAID [hasta 2] y dispositivos NIC [hasta 6]) para los que desea ver la versión de firmware.

   Aparecerán las versiones de firmware del componente seleccionado de todos los servidores en el chasis miembro seleccionado.

Configuración de varios CMC mediante RACADM

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

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

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

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

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

2. En el símbolo del sistema, escriba:

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

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

3. Modifique el archivo de configuración con un editor de texto sin formato (opcional). Cualquier carácter de formato especial en el archivo de configuración puede dañar la base de datos de RACADM.
4. Use el archivo de configuración recientemente creado para modificar un CMC de destino. En el símbolo del sistema, escriba:

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

5. Restablezca el CMC de destino que se había configurado. En el símbolo del sistema, escriba:

   ```
   racadm reset
   ```

   El subcomando `getconfig -f myfile.cfg` solicita la configuración de CMC para el CMC activo y genera el archivo **myfile.cfg**. Si es necesario, se puede cambiar el nombre de archivo o guardar el archivo en una ubicación diferente.

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

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

   El subcomando `config` carga la información en otros CMC. Server Administrator utiliza el comando `config` para sincronizar las bases de datos de usuarios y de contraseñas.

Creación de un archivo de configuración del CMC

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

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

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

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

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

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

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

  El analizador lee todos los índices del CMC para ese grupo. Todos los objetos dentro de ese grupo son modificaciones cuando el CMC se configura. Si un objeto modificado representa un índice nuevo, el índice se crea en el CMC durante la configuración.
- El usuario no puede especificar un índice deseado en un archivo **.cfg**.

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

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

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

PRECAUCIÓN: Use el subcomando `racresetcfg` para restablecer la base de datos y la configuración de la interfaz de red del CMC a sus valores predeterminados originales, y quite todos los usuarios y las configuraciones de usuario. Mientras el usuario raíz se encuentra disponible, los valores de configuración de los otros usuarios también se restablecen a los valores predeterminados.

- Si escribe `racadm getconfig -f <filename> .cfg`, el comando genera un archivo **.cfg** para la configuración actual del CMC. Este archivo de configuración se puede usar como un ejemplo y como punto de inicio para el archivo **.cfg** único.

Reglas de análisis

- Las líneas que comienzan con un carácter numeral (#) se tratan como comentarios.

  Una línea de comentario debe comenzar en la columna uno. Los caracteres "#" que se encuentren en cualquier otra columna se tratarán como caracteres #.

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

  Por ejemplo:

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

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

  El carácter inicial "[" que denota un nombre de grupo debe estar en la columna uno. Este nombre de grupo se debe especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado generan un error. Los datos de configuración se organizan en grupos tal como se define en el capítulo de propiedad de base de datos de *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX). El siguiente ejemplo muestra un nombre de grupo, un objeto y el valor de propiedad de ese objeto:

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

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

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

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

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

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

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

  ```
  racadm config -g <groupname> -o <anchored object> -i <index 1-4> <unique anchor name>
  ```

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

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

  ```
  racadm config -g <groupname> -o <objectname> -i <index 1-4> ""
  ```

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

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

  ```
  racadm getconfig -g <groupname> -i <index 1-4>
  ```

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

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

- Cuando se utiliza RACADM remoto para capturar los grupos de configuración en un archivo, si no se define una propiedad clave dentro del grupo, el grupo de configuración no se guardará como parte del archivo de configuración. Si es necesario clonar estos grupos de configuración en 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

Modificación de la dirección IP del CMC

Cuando modifique la dirección IP del CMC en el archivo de configuración, quite todas las anotaciones `<variable> = <value>` innecesarias. Solo la etiqueta del grupo de variables real con [y] permanece, incluidas las dos anotaciones `<variable> = <value>` que pertenecen al cambio de dirección IP.

Ejemplo:

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

Este archivo se actualiza de la siguiente forma:

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

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

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

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

Visualización y terminación de sesiones en el CMC

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

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

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

Para ver o terminar una sesión mediante la interfaz web:

1. En el panel izquierdo, vaya a **Descripción general del chasis** y haga clic en **Red** → **Sesiones**.
   La página **Sesiones** muestra el ID de la sesión, el nombre de usuario, la dirección IP y el tipo de sesión. Para obtener más información acerca de estas propiedades, consulte la *Ayuda en línea*.
2. Para finalizar la sesión, haga clic en **Terminar** para una sesión.

Visualización y terminación de sesiones en el CMC mediante RACADM

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

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

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

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

7

Configuración de servidores

Es posible configurar los siguientes valores de un servidor:

- Nombres de las ranuras
- Configuración de red del iDRAC
- Configuración de etiqueta LAN virtual del DRAC
- Primer dispositivo de inicio
- Servidor FlexAddress
- Recurso compartido de archivos remotos
- Configuración del BIOS mediante una copia idéntica del servidor

Configuración de nombres de las ranuras

Los nombres de las ranuras se utilizan para identificar servidores individuales. Al elegir los nombres de las ranuras, se aplican las siguientes reglas:

- Los nombres pueden contener un máximo de 15 caracteres ASCII no extendidos (códigos ASCII 32 a 126). Se permite el uso de caracteres estándar y especiales en los nombres.
- 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. `Server-1, server-1, and SERVER-1` son nombres equivalentes.
- Los nombres de las ranuras no deben comenzar con las siguientes cadenas:
  - Conmutador-
  - Ventilador-
  - PS-
  - DRAC-
  - MC-
  - Chasis
  - Cubierta-Izquierda
  - Cubierta-Derecha
  - Cubierta-Central
- Se pueden utilizar las cadenas `Server-1` a `Server-4`, pero solo para la ranura correspondiente. Por ejemplo, `Server-3` es un nombre válido para la ranura 3, pero no para la ranura 4. Observe que `Server-03` es un nombre válido para cualquier ranura.

  NOTA: Para cambiar un nombre de ranura, debe tener privilegios de **Administrador de configuración del chasis**.

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

El valor de cada nombre de ranura en la interfaz web del CMC siempre suprime cualquier cambio que se aplique al nombre para mostrar en la interfaz del iDRAC.

Para editar un nombre de ranura mediante la interfaz web del CMC:

1. En el panel izquierdo, vaya a **Descripción general del chasis → Descripción general del servidor → Configuración → Nombres de ranura**.
2. En la página **Nombres de ranura**, edite el nombre de ranura, en el campo **Nombre de ranura**.
3. Para usar el nombre de host del servidor como nombre de ranura, seleccione **Utilizar nombre de host** para la opción Nombre de ranura. Esto suprime los nombres de ranura estáticos con el nombre de host del servidor (o el nombre del sistema), si se encuentra disponible. Se requiere que el agente OMSA esté instalado en el servidor. Para obtener más información sobre el agente OMSA, consulte *Dell OpenManage Server Administrator User's Guide* (Guía del usuario de Dell OpenManage Server Administrator).
4. Para guardar la configuración, haga clic en **Aplicar**.

Para restaurar el nombre de ranura predeterminado (de SLOT-01 a SLOT-4) según la posición de la ranura del servidor) en un servidor, haga clic en **Restaurar valor predeterminado**.

Establecimiento de la configuración de red del iDRAC

Para usar esta función, debe contar con una licencia Enterprise. Puede configurar la red del iDRAC de un servidor. Puede usar los ajustes de implementación rápida QuickDeploy para configurar los ajustes predeterminados de la red del iDRAC y la contraseña raíz para los servidores que se instalen más adelante. Estos ajustes predeterminados constituyen la configuración de QuickDeploy del iDRAC.

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

Configuración de los valores de red de QuickDeploy del iDRAC

Use la configuración de QuickDeploy para establecer la configuración de la red de los servidores recién insertados.

Para activar y definir la configuración de QuickDeploy de iDRAC:

1. En el panel izquierdo, haga clic en **Descripción general del servidor → Configuración → iDRAC**.
2. En la página **Implementar el iDRAC**, en la sección **Configuración de QuickDeploy**, especifique la configuración que figura en la siguiente tabla. Para obtener más información de estos campos, consulte la *Ayuda en línea*.

Tabla 9. Configuración de QuickDeploy

Configuración	Descripción
Acción cuando el servidor está insertado	Seleccione una de las siguientes opciones de la lista: • Sin acción: no se realiza ninguna acción cuando el servidor está insertado. • Solo QuickDeploy: seleccione esta opción para aplicar los valores de configuración de la

Configuración	Descripción
	red del iDRAC cuando se inserta un servidor nuevo en el chasis. Los valores de configuración especificados para la implementación automática se usan para configurar el iDRAC nuevo, que incluye la contraseña de usuario raíz si Cambiar contraseña raíz está seleccionado. • Perfil del servidor solamente: seleccione esta opción para aplicar el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis • QuickDeploy y perfil del servidor: seleccione esta opción para aplicar primero la configuración de red del iDRAC y, a continuación, el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis. .
Definir contraseña root del iDRAC al insertar servidor	Selecciona esta opción para cambiar la contraseña raíz del iDRAC de modo que coincida con el valor ingresado en el campo **Contraseña raíz del iDRAC**, en donde está insertado un servidor.
Contraseña root del iDRAC	Cuando se seleccionan las opciones **Definir contraseña raíz del iDRAC al insertar servidor** y **QuickDeploy activada**, este valor de contraseña se asigna a la contraseña de usuario raíz del iDRAC de un servidor cuando se inserta el servidor en el chasis. La contraseña puede tener de 1 a 20 caracteres imprimibles (incluidos los espacios).
Confirmar contraseña root del iDRAC	Permite volver a escribir la contraseña que figura en el campo **Contraseña**.
Activar LAN del iDRAC	Activa o desactiva el canal de LAN del iDRAC. De forma predeterminada, esta opción está desactivada.
Activar IPv4 del iDRAC	Activa o desactiva IPv4 en el iDRAC. De forma predeterminada, esta opción está activada.
Activar la IPMI en la LAN del iDRAC	Activa o desactiva IPMI en el canal de LAN para cada iDRAC presente en el chasis. De forma predeterminada, esta opción está activada.
Activar DHCP de IPv4 del iDRAC	Activa o desactiva el DHCP para cada iDRAC presente en el chasis. Si se activa esta opción, los campos **IP de QuickDeploy**, **Máscara de subred de QuickDeploy** y **Puerta de enlace de QuickDeploy** se desactivan y no se pueden modificar debido a que se utilizará DHCP para

Configuración	Descripción
	asignar automáticamente estos valores a cada iDRAC. Para seleccionar esta opción, debe marcar la opción **Activar IPv4 del iDRAC**. La dirección IP de QuickDeploy se proporciona con dos opciones: 2 y 4.
Dirección IPv4 inicial del iDRAC (ranura 1)	Especifica la dirección IP estática del iDRAC del servidor en la ranura 1 del gabinete. La dirección IP de cada iDRAC subsiguiente se incrementa en 1 para cada ranura a partir de la dirección IP estática de la ranura 1. En el caso donde la suma de la dirección IP y del número de ranura sea mayor que la máscara de subred, se mostrará un mensaje de error. **NOTA:** La máscara de subred y la puerta de enlace no se incrementan como la dirección IP. Por ejemplo, si la dirección IP inicial es `192.168.0.250` y la máscara de subred es `255.255.0.0`, la dirección IP de QuickDeploy para la ranura 15 es `192.168.0.265`. Si la máscara de subred fuera `255.255.255.0`, se muestra el mensaje de error `QuickDeploy IPaddress range is not fully within QuickDeploy Subnet` al hacer clic en **Guardar configuración de QuickDeploy** o **Completar automáticamente con la configuración de QuickDeploy**.
Máscara de red IPv4 del iDRAC	Especifica la máscara de subred de QuickDeploy que se asigna a todos los servidores recién insertados.
Puerta de enlace IPv4 del iDRAC	Especifica la puerta de enlace predeterminada de QuickDeploy que se asigna a todos los DRAC presentes en el chasis.
Activar IPv6 del iDRAC	Activa la dirección IPv6 de cada iDRAC presente en el chasis que es compatible con IPv6.
Activar la configuración automática de IPv6 del iDRAC	Activa el iDRAC para obtener la configuración de IPv6 (dirección y longitud de prefijo) de un servidor DHCPv6 y también activa la configuración automática de dirección sin estado. De forma predeterminada, esta opción está activada.
Puerta de enlace IPv6 del iDRAC	Especifica la puerta de enlace predeterminada IPv6 para asignarla a los iDRAC. El valor predeterminado es "::".

Configuración	Descripción
Longitud del prefijo IPv6 del iDRAC	Especifica la longitud del prefijo para asignar a las direcciones IPv6 del iDRAC. El valor predeterminado es 64.

3. Haga clic en **Guardar configuración de QuickDeploy** para guardar la configuración. Si ha realizado cambios en la configuración de red del iDRAC, haga clic en **Aplicar configuración de red del iDRAC** para implementar la configuración en el iDRAC.

   La función QuickDeploy solamente se ejecuta cuando está activada y se inserta un servidor en el chasis. Si se seleccionan **Definir contraseña raíz del iDRAC al insertar servidor** y **QuickDeploy activada**, se le pedirá al usuario que utilice la interfaz LCD para permitir o impedir el cambio de la contraseña. Si existen valores de configuración de la red que difieren de la configuración actual del iDRAC, se le pedirá al usuario que acepte o rechace los cambios.

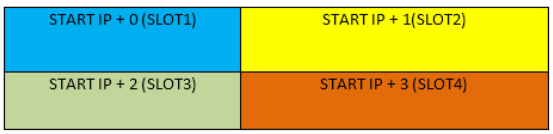
   NOTA: Cuando existe una diferencia de LAN o IPMI en LAN, el sistema le solicita al usuario que acepte el valor de dirección IP de QuickDeploy. Si la diferencia es el valor de DHCP, se le pide al usuario que acepte el valor de QuickDeploy para DHCP.

   Para copiar la configuración de QuickDeploy a la sección **Configuración de red del iDRAC**, haga clic en **Completar automáticamente con la configuración de QuickDeploy**. Los valores de configuración de red de QuickDeploy se copian en los campos correspondientes de la tabla **Valores de configuración de red del iDRAC**.

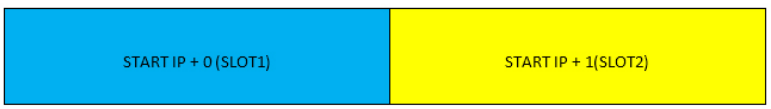
   NOTA: Los cambios realizados en los campos de QuickDeploy son inmediatos, pero es posible que para los cambios realizados en uno o más valores de configuración de la red del servidor iDRAC se necesiten varios minutos para que se propaguen del CMC al iDRAC. Si se hace clic en **Actualizar** sin esperar unos minutos, es posible que aparezcan solo los datos parcialmente correctos para uno o más servidores iDRAC.

Asignación de dirección IP de QuickDeploy para servidores

La ilustración muestra la asignación de direcciones IP de QuickDeploy a los servidores cuando existen cuatro servidores de altura media en el chasis VRTX:



La ilustración siguiente muestra la asignación de direcciones IP de QuickDeploy a los servidores cuando existen dos blades de altura media en el chasis VRTX:



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

Con esta función, es posible configurar los valores de configuración de red del iDRAC para cada servidor instalado. Los valores iniciales que se muestran para cada campo son los valores actuales leídos desde iDRAC. Para usar esta función, se debe contar con una licencia Enterprise.

Para modificar la configuración de red del iDRAC:

1. En el panel izquierdo, haga clic en **Descripción general del servidor** y, a continuación, haga clic en **Configuración**. En la página **Implementar iDRAC** se incluye la sección **Configuración de red del iDRAC** donde se muestran los valores de configuración de la red IPv4 y la red IPv6 de todos los servidores instalados.
2. Modifique la configuración de red del iDRAC según sea necesario para los servidores.

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

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

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

Modificación de la configuración de red del iDRAC mediante RACADM

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

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

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

Configuración de los valores de la etiqueta LAN virtual del iDRAC

Las etiquetas LAN virtual (VLAN) se utilizan para permitir que varias VLAN coexistan en el mismo cable de red físico y para segregar el tráfico de red por motivos de seguridad o de administración de carga. Cuando se activa la función de VLAN, se asigna una etiqueta VLAN a cada paquete de red. Las etiquetas VLAN son propiedades del chasis. Se conservan en el chasis aunque se elimine un componente.

Configuración de los valores de la etiqueta LAN virtual del iDRAC mediante RACADM

- Especifique la identificación y la prioridad de LAN virtual de un servidor específico con el siguiente comando:

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

  Los valores válidos para <*n*> son de 1 a 4.

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

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

  Por ejemplo:

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

  Por ejemplo:

- Para eliminar la VLAN de un servidor, desactive las capacidades de VLAN de la red del servidor especificado:

  ```
  racadm setniccfg -m server-<n> -v
  ```

  Los valores válidos para <*n*> son de 1 a 4.

  Por ejemplo:

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

Configuración de los valores de la etiqueta LAN virtual del iDRAC mediante la interfaz web

Para configurar la LAN virtual (VLAN) del servidor:

1. Desplácese a cualquiera de las siguientes páginas:
   - En el panel izquierdo, haga clic en **Descripción general del chasis** → **Red** → **VLAN**.
   - En el panel izquierdo, haga clic en **Descripción general del chasis** → **Descripción general del servidor** y haga clic en**Configuración** → **VLAN**.
2. En la página **Configuración de la etiqueta VLAN**, en la sección **iDRAC**, active VLAN para los servidores, establezca la prioridad e introduzca la ID. Para obtener más información sobre los campos, consulte la *ayuda en línea*.
3. Haga clic en **Aplicar** para guardar la configuración.

Configuración del primer dispositivo de inicio

Es posible especificar el primer dispositivo de inicio del CMC para cada servidor. Este puede no ser el primer dispositivo de inicio real para el servidor o incluso puede no representar un dispositivo existente en ese servidor. Representa a un dispositivo enviado por el CMC al servidor y que se utilizó como el primer dispositivo de inicio de ese servidor. Este dispositivo se puede establecer como el primer dispositivo de inicio predeterminado o un dispositivo de un solo uso, de modo que es posible iniciar una imagen para realizar tareas, como ejecutar diagnósticos o volver a instalar un sistema operativo.

Es posible configurar el primer dispositivo de inicio para el siguiente inicio solamente o para todos los reinicios subsiguientes. También puede establecer el primer dispositivo de inicio para el servidor. El

sistema se iniciará desde el dispositivo seleccionado la próxima vez que se reinicie y todas las veces subsiguientes. Ese dispositivo seguirá siendo el primer dispositivo de inicio en el orden de inicio del BIOS hasta que se vuelva a cambiar en la interfaz web del CMC (**Descripción general del chasis → Descripción general del servidor → Configuración → Primer dispositivo de inicio**) o en la secuencia de inicio del BIOS.

NOTA: La configuración del primer dispositivo de inicio en la interfaz web del CMC suprime la configuración de inicio del BIOS del sistema.

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

Es posible establecer los siguientes dispositivos para el primer inicio.

Tabla 10. Dispositivos de inicio

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

Configuración del primer dispositivo de inicio para varios servidores mediante la interfaz web del CMC

NOTA: Para configurar el primer dispositivo de inicio para los servidores, es necesario contar con privilegios de administrador **Server Administrator** o de **Administrador de configuración del chasis** y privilegios de **Inicio de sesión en el iDRAC**.

Para configurar el primer dispositivo de inicio para varios servidores:

1. En el panel izquierdo, haga clic en **Descripción general del servidor → Configuración → Primer dispositivo de inicio**. Aparecerá una lista de servidores.
2. En la columna **Primer dispositivo de inicio** del menú desplegable que corresponde al servidor, seleccione el dispositivo de inicio que desea usar para cada servidor.

3. Si desea que el servidor se inicie desde el dispositivo seleccionado cada vez que se inicie, desactive la opción **Inicio único** para el servidor. Si desea que el servidor se inicie desde el dispositivo seleccionado solamente en el siguiente ciclo de inicio, active la opción **Inicio único** para el servidor.
4. Haga clic en **Aplicar** para guardar la configuración.

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

NOTA: Para configurar el primer dispositivo de inicio para los servidores, es necesario contar con privilegios de **Server Administrator** o de **Administrador de configuración del chasis** y privilegios de **Inicio de sesión en el iDRAC**.

Para configurar el primer dispositivo de inicio para servidores individuales:

1. En el panel izquierdo, haga clic en **Descripción general del servidor** y haga clic en el servidor para el cual desea configurar el primer dispositivo de inicio.
2. Vaya a **Configuración** → **Primer dispositivo de inicio**. Se mostrará la página **Primer dispositivo de inicio**.
3. En el menú desplegable **Primer dispositivo de inicio**, seleccione el dispositivo de inicio que desea usar para cada servidor.
4. Si desea que el servidor se inicie desde el dispositivo seleccionado cada vez que se inicie, desactive la opción **Inicio único** para el servidor. Si desea que el servidor se inicie desde el dispositivo seleccionado solamente en el siguiente ciclo de inicio, active la opción **Inicio único** para el servidor.
5. Haga clic en **Aplicar** para guardar la configuración.

Configuración del primer dispositivo de inicio mediante RACADM

Para establecer el primer dispositivo de inicio, utilice el objeto `cfgServerFirstBootDevice`.

Para activar el inicio único de un dispositivo, utilice el objeto `cfgServerBootOnce`.

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

Configuración de FlexAddress para el servidor

Para obtener información acerca de cómo configurar FlexAddress para servidores, consulte Configuring FlexAddress for Chassis-Level Fabric and Slots Using CMC Web Interface (Configuración de FlexAddress para redes Fabric y ranuras en el nivel del chasis mediante la interfaz web del CMC). Para usar esta función, se debe disponer de una licencia Enterprise.

Configuración de recurso compartido de archivos remotos

La función Remote Virtual Media File Share (Recurso compartido de archivos de medios virtuales remoto) asigna un archivo de una unidad compartida en la red a uno o varios servidores mediante el CMC con el fin de implementar o actualizar un sistema operativo. Cuando se encuentra conectado, es posible obtener acceso al archivo remoto similar a un archivo al que se puede acceder en un servidor local. Se admiten dos tipos de medios: unidades de disco flexible y unidades de CD/DVD.

Para realizar una operación de recurso compartido de archivos remoto (conectarse, desconectarse o implementar), debe contar con privilegios de **Administrador de configuración del chasis** o **Administrador del servidor**. Para usar esta función, debe tener una licencia Enterprise.

Para configurar el recurso compartido de archivos remoto:

1. En el panel izquierdo, haga clic en **Descripción general del servidor → Configuración → Recurso compartido de archivos remoto**.
2. En la página **Implementar recurso compartido de archivos remoto**, escriba los datos correspondientes en los campos. Para obtener información acerca de las descripciones de los campos, consulte *Online Help* (Ayuda en línea).
3. Haga clic en **Conectar** para conectarse con un recurso compartido de archivos remoto. Para conectarse con un recurso compartido de archivos remoto, debe proporcionar la ruta de acceso, el nombre de usuario y la contraseña. Si la operación se realiza con éxito, se le permite obtener acceso a los medios.

   Haga clic en **Desconectar** para desconectarse de un recurso compartido de archivos remoto al que se conectó anteriormente.

   Haga clic en **Implementar** para implementar el dispositivo de medios.

   NOTA: Antes de hacer clic en el botón **Implementar**, asegúrese de guardar todos los archivos de trabajo, dado que esta acción reinicia el servidor.

   Cuando hace clic en **Implementar**, se ejecutan las siguientes tareas:
   - El recurso compartido de archivos remotos se conecta.
   - El archivo se selecciona como primer dispositivo de inicio de los servidores.
   - El servidor se reinicia.
   - Se suministra energía al servidor si está apagado.

Configuración de las opciones de perfil con la replicación de configuración de servidores

La función de replicación de configuración de servidores le permite aplicar todas las opciones de perfil de un servidor especificado a uno o más servidores. Las opciones de perfil que pueden replicarse son las que pueden modificarse y están pensadas para replicarse en servidores. Se muestran los siguientes tres grupos de perfiles de servidores, que pueden replicarse:

- BIOS: este grupo incluye solo la configuración del BIOS de un servidor. Estos perfiles se generan desde el CMC para PowerEdge VRTX versión 1.00 y posteriores.
- BIOS e inicio: este grupo incluye el BIOS y la configuración de inicio de un servidor. Estos perfiles se generan desde el CMC para PowerEdge VRTX versión 1.00 y posteriores.
- Todas las opciones: esta versión incluye todas las opciones de configuración del servidor y los componentes en ese servidor. Estos perfiles se generan desde
  - CMC para PowerEdge VRTX versión 1.00 y posterior
  - Servidores de 12.ª generación con iDRAC7 1.00.00 o posterior, con Lifecycle Controller 2 versión 1.1 o posterior
  - Servidores de 13.ª generación con iDRAC8 con Lifecycle Controller 2.00.00.00 o posterior

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

Para usar la función de replicación de configuración de servidores:

- Debe tener la versión mínima requerida del iDRAC.
- El servidor debe estar encendido.

Puede:

- Ver la configuración del perfil de un servidor o de un perfil guardado.
- Guardar un perfil de un servidor.
- Aplicar un perfil a otros servidores.
- Importar los perfiles almacenados desde una estación de administración o un recurso compartido de archivos remoto.
- Editar el nombre y la descripción del perfil.
- Exportar los perfiles almacenados a una estación de administración o un recurso compartido de archivos remoto.
- Eliminar perfiles guardados.
- Implementar los perfiles seleccionados en los dispositivos de destino con la opción **Implementación rápida**.
- Mostrar la actividad del registro para las tareas recientes de perfil del servidor.

Acceso a la página Perfiles de servidores

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

Para acceder a la página **Perfiles de servidores** mediante la interfaz web del CMC, en el panel izquierdo, vaya a **Descripción general del chasis** → **Descripción general del servidor**. Haga clic en **Configuración** → **Perfiles**. Aparecerá la página **Perfiles de servidores**.

Agregar o guardar perfil

Antes de clonar las propiedades de un servidor, en primer lugar capture las propiedades en un perfil almacenado. Cree un perfil almacenado e ingrese un nombre y una descripción opcional para cada perfil. Puede guardar un máximo de 16 perfiles almacenados en el soporte de almacenamiento extendido no volátil del CMC.

NOTA: Si está disponible un recurso compartido remoto, puede almacenar un máximo de 100 perfiles utilizando el almacenamiento extendido del CMC y el recurso compartido remoto. Para obtener más información sobre el recurso compartido remoto, consulte Configuración de un recurso compartido de red mediante la interfaz web del CMC.

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

Para agregar o guardar un perfil:

1. Abra la página **Perfiles del servidor**. En la sección **Perfiles del servidor**, haga clic en **Aplicar y guardar perfiles**.
2. Seleccione el servidor desde cuya configuración desee generar el perfil y, a continuación, haga clic en **Guardar perfil**.

   Aparecerá la sección **Guardar perfil**.
3. Seleccione **Almacenamiento extendido** o **Recurso compartido de red** como la ubicación en la que desea guardar el perfil.

NOTA: La opción **Recurso compartido de red** está activada y se mostrarán los detalles en la sección **Perfiles almacenados** solamente si el recurso compartido de red está montado y accesible. Si el recurso compartido de red no se encuentra conectado, configure el recurso compartido de red para el chasis. Para configurar el recurso compartido de red, haga clic en **Editar** en la sección **Perfiles almacenados**. Para obtener más información sobre cómo configurar el recurso compartido de red, consulte Configuración de un recurso compartido de red mediante la interfaz web del CMC.

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

   NOTA: Al guardar un perfil de servidor, se admite el conjunto de caracteres extendido ASCII estándar. No obstante, no se admiten los siguientes caracteres especiales:

   ), ‘, ., *, >, <, \, /, :, |, #, ?, y ,

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

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

   NOTA: El proceso de recolección de la configuración se ejecuta en segundo plano. En consecuencia, es posible que el nuevo perfil tarde algunos minutos en visualizarse. Si el nuevo perfil no se visualiza, consulte el registro del perfil para ver los errores

Aplicación de un perfil

La replicación de la configuración de servidores solamente es posible cuando existen perfiles de servidores disponibles como perfiles almacenados en el soporte no volátil del CMC o almacenados en el recurso compartido remoto. Para iniciar una operación de replicación de configuración de servidores, puede aplicar un perfil almacenado a uno o más servidores.

NOTA: Si el servidor no admite Dell Lifecycle Controller o si el chasis está apagado, no se puede aplicar un perfil al servidor.

Para aplicar un perfil a uno o varios servidores:

1. Diríjase a la página **Perfiles de servidores**. En la sección **Guardar y aplicar perfiles**, seleccione el o los servidores para los que desea aplicar el perfil seleccionado.

   Se activará el menú desplegable **Seleccionar perfil**.

   NOTA: El menú desplegable **Seleccionar perfil** muestra todos los perfiles disponibles y clasificados por tipo, incluidos aquellos que se encuentran en el recurso compartido remoto y la tarjeta SD.

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

   Se activa la opción **Aplicar perfil**.

3. Haga clic en **Aplicar perfil**.

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

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

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

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

Importar archivo

Puede importar al CMC un perfil de servidor almacenado en una estación de administración.

Para importar un perfil almacenado a partir del CMC:

1. En la página **Perfiles de servidor**, dentro de la sección **Perfiles almacenados**, haga clic en **Importar perfil**.

   Aparecerá la sección **Importar perfil de servidor**.

2. Haga clic en **Explorar** para acceder al perfil desde la ubicación requerida y luego haga clic en **Importar perfil**.

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

Exportar archivo

Puede exportar un perfil del servidor almacenado a una ruta de acceso a carpeta de archivos especificada en una estación de administración.

Para exportar un perfil almacenado:

1. Diríjase a la página **Perfiles del servidor**. En la sección **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Exportar copia del perfil**.

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

2. Haga clic en **Guardar** o **Abrir** para exportar el perfil en la ubicación requerida.

   NOTA: Si el perfil de origen está en la tarjeta SD, aparece un mensaje que le indica que si se exporta el perfil, se perderá la descripción. Presione **Aceptar** para continuar la exportación del perfil.

   Aparece un mensaje que le solicita que seleccione el destino del archivo:

   - Local o Recurso compartido de red si el archivo de origen está en una tarjeta SD.

     NOTA: Se activa la opción **Recurso compartido de red** y se muestran los detalles en la sección **Perfiles almacenados** solamente si el recurso compartido de red está montado y accesible. Si el recurso compartido de red no se encuentra conectado, configure el recurso compartido de red para el chasis. Para configurar el recurso compartido de red, haga clic en **Editar** en la sección **Perfiles almacenados**. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web del CMC.

   - Local o Tarjeta SD si el archivo de origen está en el recurso compartido de red.

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

3. Seleccione **Local**, **Almacenamiento ampliado** o **Recurso compartido de red** como ubicación de destino en función de las opciones que se muestran.

- Si selecciona **Local**, aparecerá un cuadro de diálogo que le permite guardar el perfil en un directorio local.
- Si selecciona **Almacenamiento ampliado** o **Recurso compartido de red**, se muestra el cuadro de diálogo **Guardar perfil** .

4. Haga clic en **Guardar perfil)** para guardar el perfil en la ubicación seleccionada.

Editar perfil

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

Para editar un perfil almacenado:

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

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

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

   NOTA: Puede editar la descripción del perfil solamente para los perfiles almacenados en tarjetas SD.

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

Eliminar perfil

Puede eliminar un perfil del servidor que esté almacenado en el soporte no volátil del CMC (tarjeta de SD) o en recurso compartido de red.

Para eliminar un perfil almacenado:

1. En la página **Perfiles del servidor**, en la sección **Perfiles almacenados**, seleccione el perfil requerido y haga clic en **Eliminar perfil**.

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

2. Haga clic en **Aceptar** para eliminar el perfil seleccionado.

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

Visualizar configuración de perfil

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

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

NOTA: La función Replicación de configuración de servidores del CMC recupera y muestra los valores de un servidor específico solamente si la opción **Recolectar inventario del sistema en el reinicio** (CSIOR) se encuentra activada.

Para activar la opción CSIOR en:

- Servidores de 12.ª generación: después de reiniciar el servidor, cuando el logotipo de la empresa aparece, seleccione F2. En la página **Configuración de iDRAC**, en el panel izquierdo, haga clic en **Lifecycle Controller** y, a continuación, haga clic en **CSIOR** para activar los cambios.

- Servidores de 13.ª generación: después de reiniciar el servidor, cuando se le solicite, presione F10 para acceder a Dell Lifecycle Controller. Para ir a la página de **Inventario de hardware**, seleccione **Configuración de hardware → Inventario de hardware**. En la página **Inventario de hardware**, haga clic en **Recopilar inventario del sistema al reinicio**.

Visualización de la configuración de los perfiles almacenados

Para ver la configuración de los perfiles de servidores almacenados, vaya a la página **Perfiles del servidor**. En la sección **Perfiles guardados**, haga clic en **Ver** en la columna **Ver perfil** del perfil de servidor requerido. Aparecerá la página **Ver configuración**. Para obtener más información sobre la configuración visualizada, consulte la *Ayuda en línea*.

Visualización del registro de perfiles

Para ver el registro de perfiles, en la página **Perfiles del servidor**, consulte la sección **Registro de perfiles reciente**. Esta sección enumera las 10 entradas más recientes del registro de perfiles directamente desde las operaciones de clonación de servidores. Cada entrada del registro muestra la gravedad, la fecha y la hora de envío de la operación de replicación de configuración de servidores y la descripción del mensaje de registro de replicación. Las entradas del registro también están disponibles en el registro del RAC. Para ver el resto de las entradas disponibles, haga clic en **Ir al registro de perfiles**. Aparecerá la página **Registro de perfiles**. Para obtener más información, consulte la *Ayuda en línea*.

Estado de compleción y solución de problemas

Para revisar el estado de compleción de un perfil de BIOS aplicado:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Descripción general del servidor → Configuración → Perfiles**.
2. En la página **Perfiles del servidor**, anote el valor de Identificación de trabajo (JID) para el trabajo enviado a partir de la sección **Registro de perfiles reciente**.
3. En el panel izquierdo, haga clic en **Descripción general del servidor → Solución de problemas → Trabajos en Lifecycle Controller**. Busque la misma identificación de trabajo en la tabla **Trabajos**. Para obtener más información sobre cómo realizar trabajos en Lifecycle Controller mediante el CMC, consulte las Operaciones de trabajo en Lifecycle Controller.

Implementación rápida de perfiles

La función Implementación rápida le permite asignar un perfil almacenado a una ranura del servidor. Cualquier servidor compatible con la replicación de la configuración del servidor insertado en esa ranura se configurará con el perfil asignado a dicha ranura. Puede realizar la acción Implementación rápida solamente si la opción **Acción cuando el servidor está insertado** de la página **Implementar el iDRAC** está configurado en la opción **Perfil del servidor** o la opción **Implementación rápida y perfil del servidor**. Si selecciona esta opción, podrá aplicar el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis. Para ir a la página **Implementar iDRAC** , seleccione **Descripción general de servidor → Configuración → iDRAC**. Los perfiles que pueden implementarse están almacenados en la tarjeta SD o en el recurso compartido remoto.

NOTA:

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

Asignación de perfiles del servidor a ranuras

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

1. En la página **Perfiles del servidor**, haga clic en **Perfiles para implementación rápida**.
   Aparecerán las asignaciones de perfiles actuales para las ranuras en los cuadros seleccionados en la columna **Asignar perfilr**.

   NOTA: Puede realizar la acción Implementación rápida solamente si la opción **Acción cuando el servidor está insertado** de la página **Implementar el iDRAC** está establecida en **Perfil de servidor** o en **Implementación rápida y luego el perfil del servidor**. Si se selecciona esta opción, se permite aplicar el perfil del servidor asignado cuando se inserta un nuevo servidor en el chasis.
2. En el menú desplegable, seleccione el perfil que desee asignar a la ranura requerida. Puede seleccionar perfiles para aplicarlos a varias ranuras.
3. Haga clic en **Asignar perfil**.
   El perfil se asigna a las ranuras seleccionadas.

NOTA:

- Una ranura que no tiene ningún perfil asignado se indica mediante el término "Sin perfil seleccionado" que aparece en el cuadro de selección.
- Para eliminar una asignación de perfil de una o más ranuras, seleccione las ranuras y haga clic en **Quitar asignación**. Aparece un mensaje advirtiéndole que si se quita un perfil de la ranura o las ranuras, se eliminan los valores de configuración del perfil desde los servidores que estén insertados en las ranuras cuando se activa la función **Perfiles para implementación rápida**. Haga clic en **Aceptar** para quitar las asignaciones de perfil.
- Para quitar todas las asignaciones de perfiles de una ranura, seleccione **Sin perfil seleccionado** en el menú desplegable.

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

NOTA:

- Si se encuentra un perfil asignado en el recurso compartido de red, el cual no esté accesible cuando se inserta un servidor en la ranura, la pantalla LCD muestra un mensaje que indica que el perfil asignado no está disponible para la ranura <X>.
- Se activa la opción **Recurso compartido de red** y se muestran los detalles en la sección **Perfiles almacenados** solamente si el recurso compartido de red está montado y accesible. Si el recurso compartido de red no se encuentra conectado, configure el recurso compartido de red para el chasis. Para configurar el recurso compartido de red, haga clic en **Editar** en la sección **Perfiles almacenados**. Para obtener más información, consulte Configuración de un recurso compartido de red mediante la interfaz web del CMC.

Inicio del iDRAC mediante el inicio de sesión único

El CMC proporciona una administración limitada de componentes individuales del chasis, como los servidores. Para una administración completa de estos componentes individuales, el CMC proporciona

un punto de inicio para la interfaz basada en Web de la controladora de administración del servidor (iDRAC).

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

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

  NOTA: En este contexto, el término "la misma cuenta" significa que el usuario tiene el mismo nombre de inicio de sesión con una contraseña que coincide para el CMC y para el iDRAC. Cuando el usuario tenga el mismo nombre de inicio de sesión pero no disponga de una contraseña que coincida, no se considerará que tiene la misma cuenta.

  NOTA: Se puede pedir a los usuarios que inicien sesión en el iDRAC (consulte la política de inicio de sesión único en la tercera viñeta anterior).

  NOTA: Si se desactiva la LAN de la red del iDRAC (LAN activada= No), el inicio de sesión único no estará disponible.

Si se extrae el servidor del chasis, se cambia la dirección IP del iDRAC o la conexión de red del iDRAC tiene algún problema, es posible que aparezca una página de error al hacer clic en Iniciar interfaz gráfica de usuario del iDRAC.

Inicio del iDRAC desde la página Estado del servidor

Para iniciar la consola de administración del iDRAC de un servidor individual:

1. En el panel izquierdo, expanda **Descripción general del servidor**. Los cuatro servidores aparecen en la lista expandida **Descripción general del servidor**.
2. Haga clic en el servidor para el cual desea iniciar la interfaz web del iDRAC.
3. En la página **Estado de los servidores**, haga clic en **Iniciar el iDRAC**.

   Aparece la interfaz web del iDRAC. Para obtener información acerca de las descripciones de los campos, consulte la *ayuda en línea*.

Inicio del iDRAC desde la página Estado de los servidores

Para iniciar la consola de administración del iDRAC desde la página **Estado de los servidores**, realice estos pasos:

1. En el panel izquierdo, haga clic en **Descripción general del servidor**.
2. En la página **Estado de los servidores**, haga clic en **Iniciar el iDRAC** para el servidor en el que desea iniciar la interfaz web del iDRAC.

Inicio de la consola remota

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

- El chasis está encendido.
- Servidores que admiten iDRAC7 y iDRAC8.
- La interfaz de LAN en el servidor está activada.
- El sistema host está instalado con JRE (Java Runtime Environment) 6 Update 16 o superior.
- El explorador del sistema host admite el uso de ventanas emergentes (el bloqueo de ventanas emergentes está desactivado).

La consola remota también puede iniciarse desde la interfaz web del iDRAC. Para obtener información más detallada, consulte *iDRAC User's Guide* (Guía del usuario de iDRAC) disponible en dell.com/support/manuals.

Inicio de la consola remota desde la página Condición del chasis

Para iniciar una consola remota desde la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, haga clic en **Propiedades**.
2. En la página **Condición del chasis**, haga clic en el servidor especificado en el gráfico del chasis.
3. En la sección **Vínculos rápidos**, haga clic en el vínculo **Consola remota** para iniciar la consola remota.

Inicio de la consola remota desde la página Estado del servidor

Para iniciar la consola remota de un servidor individual:

1. En el panel izquierdo, expanda la opción **Descripción general del servidor**. Los cuatro servidores aparecerán en la lista expandida de servidores.
2. Haga clic en el servidor en el que desea iniciar la consola remota.
3. En la página **Estado del servidor**, haga clic en **Iniciar la consola remota**.

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

Para iniciar la consola remota desde la página **Estado de los servidores**:

1. En el panel izquierdo, vaya a **Descripción general del servidor** y haga clic en **Propiedades** → **Estado**. Aparecerá la página **Estado de los servidores**.
2. Haga clic en **Iniciar la consola remota** para el servidor necesario.

8

Configuración del CMC para enviar alertas

Puede configurar alertas y acciones para ciertos sucesos que ocurren en el chasis. Se genera un suceso cuando el estado de un dispositivo o servicio ha cambiado o cuando se detecta una condición de error. Si un suceso coincide con un filtro de sucesos y usted ha configurado este filtro para que genere un mensaje de alerta (alerta por correo electrónico o de captura de SNMP), entonces se envía una alerta a uno o más destinos configurados como la dirección de correo electrónico, la dirección IP o un servidor externo.

Para configurar el CMC para enviar alertas:

1. Activa la opción **Alertas de sucesos del chasis**.
2. Opcionalmente, puede filtrar las alertas en función de la categoría o la gravedad.
3. Configure los valores de la alerta por correo electrónico o la captura SNMP.
4. Active las alertas de sucesos del chasis para enviar una alerta por correo electrónico o capturas SNMP a los destinos configurados.

Activación o desactivación de alertas

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

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

Activación o desactivación de alertas mediante la interfaz web del CMC

Para activar o desactivar la generación de alertas:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Alertas**.
2. En la página **Sucesos del chasis**, en la sección **Activación de alertas del chasis**, seleccione la opción **Activar alertas de sucesos del chasis** para habilitar o borrar la opción para desactivar la alerta.
3. Para guardar la configuración, haga clic en **Aplicar**.

Filtrado de alertas

Es posible filtrar las alertas por categoría y gravedad.

Filtrado de alertas mediante la interfaz web de CMC

Para filtrar las alertas según su categoría y gravedad:

NOTA: Para aplicar los cambios en la configuración de los sucesos del chasis, es necesario tener el privilegio de configuración de alertas.

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Alertas**.
2. En la página **Sucesos del chasis**, en la sección **Filtro de alertas**, seleccione una o varias de las siguientes categorías:
   - **Condición del sistema**
   - **Almacenamiento**
   - **Configuración**
   - **Auditorías**
   - **Actualizaciones**
3. Seleccione uno o más de los niveles de gravedad siguientes:
   - **Crítico**
   - **Aviso**
   - **Informativo**

   La sección **Alertas supervisadas** muestra los resultados en función de la categoría y gravedad seleccionadas. Para obtener información acerca de las descripciones de los campos en esta página, consulta la *ayuda en línea*.
4. Haga clic en **Aplicar**.

Configuración de alertas de suceso mediante RACADM

Para establecer una alerta de sucesos, ejecute el comando `eventfilters`. Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support//manuals**.

Configuración de destinos de alerta

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

Es posible configurar destinos de alerta IPv4 e IPv6, valores de correo electrónico y valores del servidor SMTP y después probar la configuración.

Antes de configurar los valores de la alerta por correo electrónico o la captura SNMP, asegúrese de tener el privilegio de Administrador de configuración del chasis.

Configuración de destinos de alerta de las capturas SNMP

Es posible configurar las direcciones IPv6 o IPv4 para la recepción de capturas SNMP.

Configuración de destinos de alerta de las capturas SNMP mediante la interfaz web del CMC

Para configurar los valores de destino de alerta IPv4 o IPv6 mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Alertas** → **Valores de captura**.
2. En la página **Destinos de alerta de sucesos del chasis**, escriba lo siguiente:

- En el campo **Destino**, especifique una dirección IP válida. Utilice el formato IPv4 de cuatro números con puntos intermedios, la notación estándar de dirección IPv6 o el nombre de dominio completo (FQDN). Por ejemplo: 123.123.123.123 o 2001:db8:85a3::8a2e:370:7334 o dell.com.

  Elija un formato que sea consistente con la infraestructura o la tecnología de red. La función Probar captura no puede detectar las elecciones incorrectas en función de la configuración de red (por ejemplo, el uso de un destino IPv6 en un entorno exclusivamente de IPv4).
- En el campo **Cadena de comunidad**, especifique un nombre de comunidad válida a la que pertenezca la estación de administración de destino.

  Esta cadena de comunidad es distinta a la que se muestra en la página **Descripción general del chasis → Red → Servicios**. La cadena de comunidad de capturas SNMP es la comunidad que CMC utiliza para las capturas de salida destinadas a las estaciones de administración. La cadena de comunidad de la página **Descripción general del chasis → Red → Servicios** es la cadena de comunidad que las estaciones de administración utilizan para consultar el daemon SNMP en el CMC.
- En **Activada**, seleccione la opción correspondiente a la dirección IP de destino para activar la dirección IP de forma que reciba las capturas. Es posible especificar hasta cuatro direcciones IP.

3. Haga clic en **Aplicar** para guardar la configuración.
4. Para probar si la dirección IP puede recibir las capturas SNMP, haga clic en **Enviar** en la columna **Probar captura SNMP**.

   Se configurarán los destinos de alerta IP.

Configuración de destinos de alerta de las capturas SNMP mediante RACADM

Para configurar los destinos de alerta IP mediante RACADM:

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

   NOTA: Solo es posible configurar una máscara de filtro para las alertas por correo electrónico y SNMP. Si ya se ha seleccionado la máscara de filtro, no realice la tarea 2 y vaya al paso 3.
2. Active la generación de alertas:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
3. Especifique los filtros de sucesos al ejecutar el comando `racadm eventfilters set`.
   a. Para borrar todas las configuraciones de alertas disponibles, ejecute el siguiente comando: `racadm eventfilters set -c cmc.alert.all -n none`
   b. Configure mediante el parámetro gravedad. Por ejemplo, todos los sucesos informativos en la categoría almacenamiento tienen asignado el apagado como acción y correo electrónico y SNMP como notificaciones: `racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`
   c. Configure mediante la subcategoría como un parámetro. Por ejemplo, todas las configuraciones bajo la subcategoría licencias en la categoría auditoría tienen asignado apagado como acción y todas las notificaciones están activadas: `racadm eventfilters set -c cmc.alert.audit.lic -n all`
   d. Configure mediante la subcategoría y gravedad como parámetros. Por ejemplo, todos los sucesos informativos en la subcategoría licencias en la categoría auditoría tienen asignado apagado como acción y todas las notificaciones están desactivadas: `racadm eventfilters set -c cmc.alert.audit.lic.info -n none`
4. Active las alertas de capturas:

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

   donde `<index>` es un valor entre 1 y 4. El CMC usa el número de índice para distinguir hasta cuatro destinos configurables para las alertas de capturas. Los destinos se pueden especificar como

direcciones numéricas con el formato apropiado (IPv6 o IPv4) o como nombres de dominio completos (FQDN).

5. Especifique una dirección IP de destino para recibir la alerta de capturas:

   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
   ```

   donde `<IP address>` es un destino válido e `<índice>` es el valor de índice que se especificó en el paso 4.

6. Especifique el nombre de comunidad:

   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i
   <index>
   ```

   donde `<community name>` es la comunidad SNMP a la que pertenece el chasis e `<index>` es el valor de índice que se especificó en los pasos 4 y 5.

   Se pueden configurar hasta cuatro destinos para recibir alertas de capturas. Para agregar más destinos, repita los pasos 2 a 6.

   NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice que se ha especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgTraps -i <index>`. Si el índice está configurado, aparecerán los valores para los objetos **cfgTrapsAlertDestIPAddr** y **cfgTrapsCommunityName**.

7. Para probar cuál es el destino de las alertas de una captura de sucesos, escriba:

   ```
   racadm testtrap -i <index>
   ```

   donde `<index>` es un valor de 1 a 4 que representa el destino de alerta que desea probar.

   Si no está seguro acerca del número de índice, ejecute el siguiente comando:

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

Configuración de los valores de alertas por correo electrónico

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

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

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

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

Si la red tiene un servidor SMTP que genera y renueva las concesiones de las direcciones IP periódicamente, y las direcciones son distintas, habrá un período durante el cual el valor de esta propiedad no funcionará debido al cambio en la dirección IP especificada del servidor SMTP. En estos casos, use el nombre DNS.

Configuración de los valores de alerta por correo electrónico mediante la interfaz web del CMC

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

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Alertas → Valores de alerta de correo electrónico**.
2. Especifique la configuración del servidor de correo electrónico SMTP y las direcciones de correo electrónico a las que se enviarán las alertas. Para obtener información acerca de las descripciones de los campos, consulte la *ayuda en línea*.
3. Haga clic en **Aplicar** para guardar la configuración.
4. Haga clic en **Enviar** en la sección **Correo electrónico de prueba** para enviar un correo electrónico de prueba al destino de alerta por correo electrónico especificado.

Configuración de los valores de alerta por correo electrónico mediante RACADM

Para enviar un correo electrónico de prueba a un destino de alerta por correo electrónico mediante RACADM:

1. Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
2. Active la generación de alertas:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```

   NOTA: Solo puede configurarse una máscara de filtro en las alertas por correo electrónico y captura SNMP. Si ya configuró una máscara de filtro, no ejecute la tarea del paso 3.
3. Especifique los sucesos para los que se deben generar alertas:

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
   ```

   en donde `<mask value>` es un valor hexadecimal entre 0x0 y 0xffffffff que se debe expresar con los caracteres iniciales 0x. En la tabla Máscaras de filtro para capturas de sucesos se proporcionan máscaras de filtro para cada tipo de suceso. Para obtener instrucciones acerca de la forma de calcular el valor hexadecimal para la máscara de filtro que desea activar, consulte el paso 3 en Configuración de destinos de alerta de las capturas SNMP mediante RACADM.
4. Active la generación de alertas por correo electrónico:

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

   en donde `<index>` es un valor entre 1 y 4. El CMC usa el número de índice para distinguir hasta cuatro direcciones de correo electrónico de destino que pueden configurarse.
5. Especifique una dirección de correo electrónico de destino para recibir las alertas por correo electrónico:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i
   <index>
   ```

   donde `<email address>` es una dirección de correo electrónico válida e `<index>` es el valor del índice que se especificó en el paso 4.
6. Especifique el nombre de la persona que recibirá la alerta por correo electrónico:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i
   <index>
   ```

   donde `<email name>` (<nombre de correo electrónico>) es el nombre de la persona o el grupo que recibirá la alerta por correo electrónico e `<index>` (<índice>) es el valor del índice que se especificó

en los pasos 4 y 5. El nombre de correo electrónico puede contener hasta 32 caracteres alfanuméricos, guiones, guiones bajos y puntos. Los espacios no son válidos.

7. Configure el host SMTP:

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
   ```

   donde `host.domain` (host.dominio) es el nombre de dominio completo.

   Puede configurar hasta cuatro direcciones de correo electrónico de destino para recibir las alertas por este medio. Para agregar más direcciones, ejecute las tareas de los pasos 2 a 6.

   NOTA: Los comandos que se indican en los pasos 2 a 6 sobrescriben todos los valores configurados para el índice que se ha especificado (1 a 4). Para determinar si un índice tiene valores configurados previamente, escriba: `racadm getconfig -g cfgEmailAlert — I <index>`. Si el índice está configurado, aparecerán los valores para los objetos cfgEmailAlertAddress y cfgEmailAlertEmailName.

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

9

Configuración de cuentas de usuario y privilegios

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

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

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

Tipos de usuarios

Hay dos tipos de usuarios:

- Usuarios del CMC o usuarios del chasis
- Usuarios del iDRAC o usuarios del servidor (dado que el iDRAC reside en un servidor)

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

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

Tabla 11. Tipos de usuarios

Privilegio	Descripción
Usuario con acceso al CMC	El usuario puede iniciar sesión en el CMC y ver todos los datos del CMC, pero no puede agregar o modificar datos ni ejecutar comandos.

Privilegio	Descripción
	Es posible que un usuario tenga otros privilegios sin el privilegio de Usuario con acceso al CMC. Esta función es útil cuando no se le permite iniciar sesión temporalmente a un usuario. Cuando el privilegio de Usuario con acceso al CMC de ese usuario se restablece, el usuario conserva todos los demás privilegios otorgados anteriormente.
Administrador de configuración del chasis	El usuario puede agregar o cambiar los datos que: • Identifican el chasis, como el nombre y la ubicación del chasis. • Están asignados específicamente al chasis, como el modo IP (estático o DHCP), la dirección IP estática, la puerta de enlace estática y la máscara de subred estática. • Brindan servicios al chasis, como la fecha y la hora, la actualización de firmware y el restablecimiento del CMC. • Se relacionan con el chasis, como el nombre de ranura y la prioridad de ranura. Aunque estas propiedades se aplican a los servidores, se trata estrictamente de propiedades del chasis que se relacionan con las ranuras y no con los servidores en sí. Por este motivo, los nombres y las prioridades de ranura se pueden agregar o cambiar sin importar si los servidores están presentes en las ranuras. Cuando un servidor se mueve a otro chasis, hereda el nombre de ranura y la prioridad asignada a la ranura correspondiente en el nuevo chasis. El nombre y la prioridad de ranura anteriores se conservan en el chasis anterior. NOTA: Los usuarios del CMC que tienen el privilegio de **Administrador de configuración del chasis** pueden configurar los valores de alimentación. Sin embargo, el privilegio de **Administrador de control del chasis** es necesario para realizar operaciones de alimentación del chasis, como el encendido, el apagado y el ciclo de encendido.
Administrador de configuración de usuarios	El usuario puede: • Agregar un nuevo usuario. • Cambiar la contraseña de un usuario. • Cambiar los privilegios de un usuario. • Activar o desactivar el privilegio de inicio de sesión de un usuario pero conservar el nombre y otros privilegios del usuario en la base de datos.
Administrador de borrado de registros	El usuario puede borrar los registros de hardware y del CMC.
Administrador de control del chasis (comandos de alimentación)	Los usuarios del CMC con privilegios de **Administrador de alimentación del chasis** pueden realizar todas las operaciones relacionadas con la administración de alimentación. Pueden controlar las operaciones de alimentación del chasis, como el encendido, el apagado y el ciclo de encendido. NOTA: Para configurar los valores de alimentación, es necesario el privilegio de **Administrador de configuración del chasis**.

Privilegio	Descripción
Server Administrator	Se trata de un privilegio general que otorga al usuario del CMC todos los derechos para realizar cualquier operación en los servidores que estén presentes en el chasis. Cuando un usuario con el privilegio de administrador **Server Administrator** genera una acción que se debe realizar en un servidor, el firmware del CMC envía el comando al servidor de destino sin verificar los privilegios del usuario en el servidor. Es decir, el privilegio de **Server Administrator** anula la falta de privilegios de administrador en el servidor. Sin el privilegio de **Server Administrator**, los usuarios que se hayan creado en el chasis solo pueden ejecutar un comando en un servidor cuando se cumplan todas las condiciones siguientes: • El mismo nombre de usuario existe en el servidor. • El mismo nombre de usuario debe tener la misma contraseña en el servidor. • El usuario debe tener privilegios para ejecutar el comando. Cuando un usuario del CMC que no tiene privilegios de **Server Administrator** genera una acción que se debe ejecutar en un servidor, el CMC envía un comando al servidor de destino con el nombre y la contraseña de inicio de sesión del usuario. Si el usuario no existe en el servidor o la contraseña no coincide, se negará al usuario la capacidad de ejecutar la acción. Si el usuario existe en el servidor de destino y la contraseña coincide, el servidor responderá según los privilegios que el usuario tenga en el servidor. En función de los privilegios que se tengan en el servidor, el firmware del CMC decidirá si el usuario tiene derecho de ejecutar la acción. A continuación se muestra una lista de los privilegios y las acciones en el servidor a los que se tiene derecho con el privilegio de Server Administrator. Estos derechos se aplican únicamente cuando el usuario del chasis no tiene privilegios de Administrador del servidor en el chasis. Administrador de configuración del servidor: • Establecer dirección IP • Establecer puerta de enlace • Establecer máscara de subred • Establecer primer dispositivo de inicio Configurar usuarios: • Establecer contraseña raíz del iDRAC • Restablecimiento de iDRAC Administrador de control del servidor: • Encendido • Apagado • Ciclo de encendido • Apagado ordenado

Privilegio	Descripción
	• Reinicio del servidor
Usuario de alertas de prueba	El usuario puede enviar mensajes de alerta de prueba.
Administrador de comandos de depuración	El usuario puede ejecutar comandos de diagnóstico del sistema.
Administrador de red Fabric A	El usuario puede definir y configurar el módulo de E/S de la red Fabric A.
Administrador de red Fabric B	El usuario puede definir y configurar la red Fabric B que corresponde a la primera tarjeta mezzanine de los servidores y está conectada al circuito de la red Fabric B en el subsistema PCIe compartido en la placa principal.
Administrador de red Fabric C	El usuario puede definir y configurar la red Fabric C que corresponde a la segunda tarjeta mezzanine de los servidores y está conectada al circuito de la red Fabric C en el subsistema PCIe compartido en la placa principal.

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

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

Tabla 12. Privilegios del grupo del CMC

Grupo de usuarios	Privilegios otorgados
Administrador	• Usuario con acceso al CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Server Administrator • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A
Usuario avanzado	• Inicio de sesión • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Server Administrator • Usuario de alertas de prueba • Administrador de red Fabric A
Usuario invitado	Inicio de sesión
Personalizar	Seleccione cualquier combinación de los siguientes permisos: • Usuario con acceso al CMC

Grupo de usuarios	Privilegios otorgados
	• Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Server Administrator • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A
Ninguno	Sin permisos asignados

Tabla 13. Comparación de los privilegios entre administradores, usuarios avanzados y usuarios invitados del CMC

Conjunto de privilegios	Permisos de administrador	Permisos de usuario avanzado	Permisos de usuario invitado
Usuario con acceso al CMC	Sí	Sí	Sí
Administrador de configuración del chasis	Sí	No	No
Administrador de configuración de usuarios	Sí	No	No
Administrador de borrado de registros	Sí	Sí	No
Administrador de control del chasis (comandos de alimentación)	Sí	Sí	No
Server Administrator	Sí	Sí	No
Usuario de alertas de prueba	Sí	Sí	No
Administrador de comandos de depuración	Sí	No	No
Administrador de red Fabric A	Sí	Sí	No

Modificación de la configuración de cuentas raíz de administración para usuarios

Para una mayor seguridad, se recomienda cambiar la contraseña predeterminada de la cuenta root (Usuario 1). La cuenta root es la cuenta de administración predeterminada que se envía con el CMC.

Para cambiar la contraseña predeterminada para la cuenta raíz:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, en **Autentificación de usuario**.
2. En la página **Usuarios**, en la columna **ID de usuario**, haga clic en **1**.

   NOTA: ID de usuario **1** es la cuenta de usuario raíz que se envía con el CMC. Este valor no se puede modificar.
3. En la página **Configuración de usuario**, seleccione la opción **Cambiar contraseña**.
4. Escriba la nueva contraseña en el campo **Contraseña** y, a continuación, escriba la misma contraseña en **Confirmar contraseña**.
5. Haga clic en **Aplicar**. La contraseña se cambia por la ID de de usuario **1**.

Configuración de usuarios locales

Es posible configurar hasta 16 usuarios locales en el CMC con privilegios de acceso específicos. Antes de crear un usuario local para el CMC, compruebe si existen usuarios actuales. Puede establecer nombres de usuario, contraseñas y funciones con privilegios para estos usuarios. Los nombres de usuario y las contraseñas se pueden cambiar mediante cualquiera de las interfaces seguras del CMC (es decir, la interfaz web, RACADM o WS-MAN).

Configuración de los usuarios locales mediante la interfaz web del CMC

NOTA: Es necesario contar con el permiso **Configurar usuarios** para poder crear un usuario del CMC.

Para agregar y configurar usuarios locales en el CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** y, a continuación, en **Autentificación de usuario**.
2. En la página **Usuarios locales**, en la columna **ID de usuario**, haga clic en un número de ID de usuario. Aparece la página **Configuración de usuario**.

   NOTA: ID de usuario 1 es la cuenta de usuario raíz que se envía con el CMC. Este valor no se puede modificar.
3. Active la ID de usuario y especifique el nombre de usuario, la contraseña y los privilegios de acceso del usuario. Para obtener más información acerca de las opciones, consulte la *ayuda en línea*.
4. Haga clic en **Aplicar**. El usuario se crea con los privilegios adecuados.

Configuración de los usuarios locales mediante RACADM

NOTA: Se debe haber iniciado sesión como usuario `root` para ejecutar los comandos RACADM en un sistema remoto con Linux.

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

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

NOTA: Los usuarios se pueden activar y desactivar con el tiempo y la desactivación de un usuario no lo borra de la base de datos.

Para verificar si un usuario existe, abra una consola de texto de Telnet/SSH en el CMC, inicie sesión y escriba el siguiente comando una vez para cada índice de 1 a 16:

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

NOTA: También puede escribir `racadm getconfig -f <myfile.cfg>` y ver o editar el archivo **myfile.cfg**, que incluye todos los parámetros de configuración del CMC.

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

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

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

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

El carácter "#" en los objetos de comando indica que es un objeto de solo lectura. Asimismo, si utiliza el comando `racadm config -f racadm.cfg` para especificar cualquier número de grupos u objetos para escribir, no se puede especificar el índice. Un usuario nuevo se agrega al primer índice disponible. Este comportamiento permite una mayor flexibilidad a la hora de configurar un segundo CMC con los mismos valores que el CMC principal.

Adición de un usuario del CMC mediante RACADM

Para agregar un usuario nuevo a la configuración del CMC:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca los privilegios de usuario. Para obtener más información sobre los privilegios de usuario, consulte Types of Users (Tipos de usuarios).
4. Active el usuario.

Ejemplo:

En el siguiente ejemplo se describe la forma de agregar un nuevo usuario de nombre "John" con la contraseña "123456" y privilegios de inicio de sesión en el CMC.

NOTA: Para obtener una lista de valores de máscara de bits válidos para privilegios de usuario específicos, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX). El valor de privilegio predeterminado es 0, lo cual indica que los privilegios de un usuario no están activados.

```
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 correctamente con los privilegios adecuados, ejecute el siguiente comando:

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

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

Desactivación de un usuario del CMC

Al usar RACADM, los usuarios se deben desactivar manualmente y de manera individual. Los usuarios no se pueden eliminar mediante un archivo de configuración.

Para eliminar un usuario del CMC, la sintaxis de comando es:

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <índice>"" racadm
config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

Una cadena nula de dos caracteres de comillas ("") indica al CMC que debe eliminar la configuración de usuario en el índice especificado y restablecer los valores predeterminados originales de fábrica en la configuración de usuario.

Activación de un usuario del CMC con permisos

Para activar un usuario con permisos administrativos específicos (autoridad basada en funciones):

1. Busque un índice de usuario disponible mediante la sintaxis de comando siguiente:
   ```
   racadm getconfig -g cfgUserAdmin -i <índice>
   ```
2. Escriba los comandos siguientes con el nombre de usuario y la contraseñas nuevos.
   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <índice> <valor
   de máscara de bits de privilegio del usuario>
   ```

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

Configuración de usuarios de Active Directory

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

NOTA: En los siguientes sistemas operativos, puede reconocer a los usuarios de CMC mediante Active Directory.

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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

Mecanismos de autentificación compatibles de Active Directory

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

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

Descripción general del esquema estándar de Active Directory

Como se muestra en la figura a continuación, el uso del esquema estándar para la integración de Active Directory requiere una configuración tanto en Active Directory como en el CMC.

En Active Directory, un objeto de grupo estándar se utiliza como grupo de funciones. Un usuario con acceso al CMC es miembro del grupo de funciones. Para conceder a este usuario acceso a una tarjeta CMC específica, el nombre del grupo de funciones y su nombre de dominio deben configurarse en la tarjeta CMC específica. La función y el nivel de privilegios se definen en cada tarjeta CMC y no en Active Directory. Puede configurar hasta cinco grupos de funciones en cada CMC. En la tabla siguiente se muestran los privilegios predeterminados del grupo de funciones.

Tabla 14. : Privilegios predeterminados del grupo de funciones

Grupo de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
1	Ninguno	• Usuario con acceso al CMC • Administrador de configuración del chasis • Administrador de configuración de usuarios • Administrador de borrado de registros • Administrador de control del chasis (comandos de alimentación) • Server Administrator • Usuario de alertas de prueba • Administrador de comandos de depuración • Administrador de red Fabric A	0x00000fff
2	Ninguno	• Usuario con acceso al CMC • Administrador de borrado de registros	0x00000ed9

Grupo de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
		• Administrador de control del chasis (comandos de alimentación) • Server Administrator • Usuario de alertas de prueba • Administrador de red Fabric A	
3	Ninguno	Usuario con acceso al CMC	0x00000001
4	Ninguno	Sin permisos asignados	0x00000000
5	Ninguno	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits se utilizan únicamente cuando se establece el esquema estándar con RACADM.

NOTA: Para obtener más información sobre los privilegios de usuario, consulte Tipos de usuarios.

Configuración del esquema estándar de Active Directory

Para configurar el CMC para un acceso de inicio de sesión de Active Directory:

1. En un servidor de Active Directory (controladora de dominio), abra el complemento **Usuarios y equipos de Active Directory**.
2. Mediante la interfaz web del CMC o RACADM:
   a. Cree un grupo o seleccione un grupo existente.
   b. Configure los privilegios de funciones.
3. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para obtener acceso al CMC.

Configuración de Active Directory con esquema estándar mediante la interfaz web del CMC

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

1. En el árbol del sistema, vaya a **Descripción general del chasis** y haga clic en **Autentificación de usuario → Servicios de directorio**. Aparecerá la página **Servicios de directorio**.
2. Seleccione **Microsoft Active Directory (Esquema estándar)**. Los valores que se deben configurar para el esquema estándar se muestran en la misma página.
3. En la sección **Valores comunes**, especifique lo siguiente:
   - Seleccione **Activar Active Directory** e introduzca el valor de tiempo de espera para Active Directory en el campo **Tiempo de espera de AD** .
   - Para obtener las controladoras de dominio de Active Directory de una búsqueda en el DNS, seleccione **Buscar controladoras de dominio con DNS** y, a continuación, seleccione una de las opciones siguientes:
     – **Dominio de usuario desde inicio de sesión**: para realizar una búsqueda en el DNS con el nombre de dominio del usuario de inicio de sesión.

– **Especificar un dominio**: introduzca el nombre del dominio para utilizar en la búsqueda en el DNS.

- Para activar el CMC y utilizar las direcciones del servidor de la controladora de dominio de Active Directory especificadas, seleccione **Especificar direcciones de la controladora de dominio**. Estas direcciones del servidor son las direcciones de las controladoras de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

4. Haga clic en **Aplicar** para guardar la configuración.

   NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.

5. En la sección **Grupos de funciones del esquema estándar**, haga clic en un **Grupo de funciones**. Aparecerá la página **Configurar grupo de funciones**.
6. Especifique el nombre del grupo, el dominio y los privilegios para el grupo de funciones.
7. Haga clic en **Aplicar** para guardar la configuración del grupo de funciones y haga clic en **Volver a la página de configuración**.
8. Si ha activado la validación de certificados, debe cargar en el CMC el certificado firmado por una autoridad de certificados raíz para el bosque de dominio. En la sección **Administrar certificados**, escriba la ruta de acceso del archivo o busque el archivo de certificado. Haga clic en **Cargar** para cargar el archivo en el CMC.

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

   Los certificados SSL para las controladoras de dominio deben estar firmados por el certificado con la firma de la autoridad de certificados raíz. El certificado con la firma de la autoridad de certificados raíz debe estar disponible en la estación de administración que tiene acceso al CMC.
9. Si ha activado el inicio de sesión único (SSO), en la sección **Archivo keytab de Kerberos**, haga clic en **Examinar**, especifique el archivo keytab y haga clic en **Cargar**. Una vez completada la carga, se mostrará un mensaje donde se indicará si la carga se ha realizado correctamente o ha fallado.
10. Haga clic en **Aplicar**. El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.
11. Cierre sesión y luego inicie sesión en el CMC para completar la configuración de Active Directory en el CMC.
12. Seleccione **Chasis** en el árbol del sistema y desplácese hasta la ficha **Red**. Aparecerá la página **Configuración de la red**.
13. En **Configuración de la red**, si la opción **Usar DHCP (para la dirección IP de la interfaz de red del CMC)** está seleccionada, seleccione **Usar DHCP para obtener dirección de servidor DNS**.

    Para introducir manualmente una dirección IP del servidor DNS, desactive **Usar DHCP para obtener direcciones de servidor DNS** y escriba las direcciones IP del servidor DNS principal y alternativo.
14. Haga clic en **Aplicar cambios**.

    De esta forma, se completa la configuración de la función de Active Directory de esquema estándar para el CMC.

Configuración de Active Directory con esquema estándar vía RACADM

En el símbolo del sistema racadm, ejecute los comandos siguientes:

- Mediante el comando **config**:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 2 racadm config -g cfgStandardSchema -i
```

```
<index> -o cfgSSADRoleGroupName <common name of the role group> racadm
config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully
qualified domain name> racadm config -g cfgStandardSchema -i <index> -o
cfgSSADRoleGroupPrivilege <Bit Mask Value for specific RoleGroup
permissions>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully
qualified domain name or IP address of the domain controller> racadm
config -g cfgActiveDirectory -o cfgADDomainController2 <fully qualified
domain name or IP address of the domain controller> racadm config -g
cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain name
or IP address of the domain controller>
```

NOTA: Introduzca el FQDN de la controladora de dominio, no el FQDN del dominio. Por ejemplo, introduzca `servername.dell.com` en lugar de `dell.com`.

NOTA:
Al menos una de las tres direcciones se debe configurar. CMC intenta conectar cada una de las direcciones configuradas una a la vez hasta que establezca una conexión correcta. Con el esquema estándar, estas son las direcciones de las controladoras de dominio en las que se encuentran las cuentas de usuario y los grupos de funciones.

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <fully
qualified domain name or IP address of the domain controller> racadm
config -g cfgActiveDirectory -o cfgADGlobalCatalog2 <fully qualified
domain name or IP address of the domain controller> racadm config -g
cfgActiveDirectory -o cfgADGlobalCatalog3 <fully qualified domain name or
IP address of the domain controller>
```

NOTA:
El servidor de catálogo global solo se requiere para el esquema estándar cuando las cuentas de usuario y los grupos de roles se encuentran en dominios distintos. En el caso de dominio múltiple, solamente se puede usar el grupo universal.

NOTA:
La dirección IP o el FQDN que especifique en este campo debe concordar con el campo Sujeto o Nombre alternativo de sujeto del certificado de controladora de dominio si tiene activada la validación de certificados.

Si desea desactivar la validación de certificados durante el protocolo de enlace con SSL, ejecute el siguiente comando RACADM:

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`

En este caso, no es necesario cargar el certificado de la autoridad de certificados (CA).

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

- Mediante el comando **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`

En este caso, también debe cargar el certificado de CA con el siguiente comando de RACADM:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN de catálogo global. Asegúrese de que el DNS esté configurado correctamente.

Descripción general del esquema extendido de Active Directory

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

Extensiones de esquema de Active Directory

Los datos de Active Directory forman una base de datos distribuida de *atributos* y *clases*. El esquema de Active Directory incluye las reglas que determinan los tipos de datos que se pueden agregar o incluir en la base de datos. Un ejemplo de una clase que se almacena en la base de datos es la clase usuario. Algunos ejemplos de los atributos de la clase usuario son el nombre, el apellido, el número de teléfono y otros datos del usuario.

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

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

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

Descripción general sobre las extensiones de esquema

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

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

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

El objeto del dispositivo de RAC es el vínculo con el firmware de RAC para consultar a Active Directory con fines de autentificación y autorización. Cuando se agrega un RAC a la red, el administrador debe

configurar el RAC y su objeto de dispositivo con el nombre de Active Directory, de modo que los usuarios puedan realizar la autentificación y la autorización con Active Directory. Además, el administrador debe agregar el RAC a por lo menos un objeto de asociación para que los usuarios se puedan autentificar.

NOTA: El objeto de privilegio de RAC se aplica al CMC.

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

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

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

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

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

1. Cree dos objetos de asociación.
2. Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representen a los dos CMC.
3. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tenga todos los privilegios (de administrador) y Priv2 tenga el privilegio de inicio de sesión.
4. Agrupe usuario1 y usuario2 en grupo1.
5. Agregue Group1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objeto de privilegio en A01, y RAC1 y RAC2 como dispositivos de RAC en A01.
6. Agregue User3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objeto de privilegio en A02, y RAC2 como dispositivo de RAC en A02.

Para configurar los objetos en un escenario de varios dominios:

1. Asegúrese de que la función de bosque del dominio esté en el modo Nativo o Windows 2003.
2. Cree dos objetos de asociación, A01 (de ámbito universal) y A02, en cualquier dominio. En la figura Configuración de objetos de Active Directory en varios dominios se muestran los objetos en dominio2.
3. Cree dos objetos de dispositivo de RAC, RAC1 y RAC2, que representen a los dos CMC.
4. Cree dos objetos de privilegio, Priv1 y Priv2, donde Priv1 tenga todos los privilegios (de administrador) y Priv2 tenga el privilegio de inicio de sesión.
5. Agrupe user1 y user2 en Grup1. El ámbito de grupo de Grup1 debe ser Universal.
6. Agregue Group1 como miembro en el objeto de asociación 1 (A01), luego Priv1 como objeto de privilegio en A01, y RAC1 y RAC2 como dispositivos de RAC en A01.
7. Agregue User3 como miembro en el objeto de asociación 2 (A02), luego Priv2 como objeto de privilegio en A02, y RAC2 como dispositivo de RAC en A02.

Configuración del esquema extendido de Active Directory

Para configurar Active Directory para obtener acceso al CMC:

1. Amplíe el esquema de Active Directory.
2. Amplíe el complemento Usuarios y equipos de Active Directory.
3. Agregue usuarios del CMC y sus privilegios en Active Directory.
4. Active SSL en cada una de las controladoras de dominio.
5. Configure las propiedades de Active Directory para el CMC mediante la interfaz web del CMC o de RACADM.

Extensión del esquema de Active Directory

Extender el esquema de Active Directory agrega una unidad organizacional de Dell, clases y atributos de esquema y privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender el esquema, asegúrese de disponer los privilegios de administrador de esquemas en propietario del rol FSMO (operación maestra única flexible del esquema maestro) del bosque de dominios.

Puede extender el esquema por medio de uno de los siguientes métodos:

- Utilidad Dell Schema Extender
- Archivo de secuencia de comandos LDIF

Si utiliza el archivo de secuencia de comandos LDIF, la unidad organizacional de Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation (Herramientas y documentación de Dell Systems Management)*, en los siguientes directorios respectivos:

- Unidad de DVD:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\LDIF_Files
- <Unidad de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools \Remote_Management_Advanced\Schema Extender

Para usar los archivos LDIF, consulte las instrucciones en las notas de publicación que se incluyen en el directorio LDIF_Files.

Puede copiar y ejecutar Schema Extender o los archivos LDIF desde cualquier ubicación.

Uso de Dell Schema Extender

PRECAUCIÓN: Dell Schema Extender utiliza el archivo SchemaExtenderOem.ini. Para asegurarse de que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la **Welcome (Bienvenida)**, haga clic en **Siguiente**.
2. Lea y comprenda la advertencia y haga clic en **Siguiente**.
3. Seleccione **Usar las credenciales de inicio de sesión actuales** o introduzca un nombre de usuario y una contraseña con derechos de administrador de esquema.
4. Haga clic en **Siguiente** para ejecutar Dell Schema Extender.
5. Haga clic en **Terminar**.

   El esquema se extenderá. Para verificar la extensión del esquema, utilice el complemento de esquema de Active Directory y el MMC para verificar que las clases y los atributos existan. Para

obtener más información sobre las clases y los atributos, consulte Classes and Attributes (Clases y atributos). Para obtener detalles sobre el uso del complemento de esquema de Active Directory y el MMC, consulte la documentación de Microsoft.

Clases y atributos

Tabla 15. Definiciones de clases para las clases agregadas al esquema de Active Directory

Nombre de la clase	Número de identificación de objeto asignado (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabla 16. Clase dellRacDevice

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

Tabla 17. Clase delliDRACAssociationObject

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

Tabla 18. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (derechos de autorización) para el dispositivo CMC.
Tipo de clase	Clase auxiliar
SuperClasses	Ninguno
Atributos	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tabla 19. Clase dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Descripción	Esta clase se usa como una clase de contenedor para los privilegios de Dell (derechos de autorización).
Tipo de clase	Clase estructural
SuperClasses	User (Usuario)
Atributos	dellRAC4Privileges

Tabla 20. Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
SuperClasses	Equipo
Atributos	dellAssociationMembers

Tabla 21. Lista de atributos agregados al esquema de Active Directory

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Atributo: `dellPrivilegeMember`	FALSO

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Descripción: lista de objetos `dellPrivilege` que pertenecen a este atributo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.1 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Atributo: `dellProductMembers` **Descripción**: lista de objetos `dellRacDevices` que pertenecen a esta función. Este atributo es el vínculo de avance para el vínculo de retroceso `dellAssociationMembers.` **Identificación de vínculo**: 12070 **OID**: 1.2.840.113556.1.8000.1280.1.1.2.2 **Nombre distintivo**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellIsCardConfigAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de configuración de tarjeta en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.4 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsLoginUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de inicio de sesión en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.3 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsUserConfigAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de configuración de usuario en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.5 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `delIsLogClearAdmin`	VERDADERO

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
Descripción: el valor es VERDADERO si el usuario tiene derechos de administrador de borrado de registros en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Atributo: `dellIsServerResetUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos para restablecer el servidor en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.7 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsTestAlertUser` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de usuario de alertas de prueba en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.10 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellIsDebugCommandAdmin` **Descripción**: el valor es VERDADERO si el usuario tiene derechos de administrador de comandos de depuración en el dispositivo. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.11 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
Atributo: `dellSchemaVersion` **Descripción**: se utiliza la versión de esquema actual para actualizar el esquema. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.12 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
Atributo: `dellRacType` **Descripción**: este atributo representa el tipo de RAC actual para el objeto dellRacDevice y el	VERDADERO

OID asignado/Identificador de objeto de sintaxis	Con un solo valor
vínculo de retroceso al vínculo de avance dellAssociationObjectMembers. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.13 Cadena de no distinguir mayúsculas de minúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
Atributo: `dellAssociationMembers` **Descripción**: lista de los objetos dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el vínculo de retroceso para el atributo vinculado dellProductMembers. **Identificación de vínculo**: 12071 **OID:** 1.2.840.113556.1.8000.1280.1.1.2.14 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
Atributo: `dellPermissionsMask1` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.1 número entero (LDAPTYPE_INTEGER)	
Atributo: `dellPermissionsMask2` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.2 número entero (LDAPTYPE_INTEGER)	

Instalación de Dell Extension para el complemento Usuarios y equipos de Active Directory

Cuando se extiende el esquema en Active Directory, también debe extenderse el complemento Usuarios y equipos de Active Directory para que el administrador pueda administrar los dispositivos de RAC (CMC), los usuarios y grupos de usuarios, así como las asociaciones y los privilegios del RAC.

Cuando se instala el software de administración de sistemas mediante el DVD de *Documentación y herramientas de Dell Systems Management*, es posible extender el complemento seleccionando la opción **Complemento Usuarios y equipos de Active Directory** durante el procedimiento de instalación. Consulte la *Guía de instalación rápida del software Dell OpenManage* para obtener instrucciones adicionales acerca de la instalación del software de administración de sistemas. Para los sistemas operativos Windows de 64 bits, el instalador del complemento se encuentra en: **<DVDdrive>:\SYSMGMT \ManagementStation\support\OMActiveDirect ory_SnapIn64**.

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

Agregar usuarios y privilegios del CMC a Active Directory

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

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

Creación de un objeto de dispositivo de RAC

Para crear un objeto de dispositivo de RAC:

1. En la ventana **Raíz de consola de MMC**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo → Opciones avanzadas del objeto Dell Remote Management**.
3. En la página **Nuevo objeto**, escriba un nombre para el objeto nuevo. El nombre debe ser idéntico al nombre del CMC que se introduce en la configuración de Active Directory con el esquema estándar mediante la interfaz web.
4. Seleccione **Objeto de dispositivo de RAC** y haga clic en **Aceptar**.

Creación de un objeto de privilegio

Para crear un objeto de privilegio:

NOTA: Debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola de MMC**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo → Opciones avanzadas del objeto Dell Remote Management**.
3. En la página **Nuevo objeto**, escriba un nombre para el objeto nuevo.
4. Seleccione **Objeto de privilegio** y haga clic en **Aceptar**.
5. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
6. Haga clic en la ficha **Privilegios de RAC** y asigne los privilegios para el usuario o grupo. Para obtener más información sobre los privilegios de usuario del CMC, consulte Types of Users (Tipos de usuarios).

Creación de un objeto de asociación

El objeto de asociación deriva de un grupo y debe contener un tipo de grupo. El ámbito de asociación especifica el tipo de grupo de seguridad para el objeto de asociación. Cuando cree un objeto de asociación, seleccione el ámbito de asociación que se aplica al tipo de objeto que desea agregar. Si selecciona Universal, por ejemplo, los objetos de asociación solamente estarán disponibles cuando Active Directory Domain esté funcionando en modo nativo o en un modo superior.

Para crear un objeto de asociación:

1. En la ventana **Raíz de consola (MMC)**, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo → Opciones avanzadas del objeto Dell Remote Management**.
3. En la página **Nuevo objeto**, escriba un nombre para el objeto nuevo y seleccione **Objeto de asociación**.
4. Seleccione el ámbito para **Objeto de asociación** y haga clic en **Aceptar**.

Adición de objetos a un objeto de asociación

Mediante la ventana **Propiedades de objeto de asociación**, es posible asociar usuarios o grupos de usuarios, objetos de privilegio y dispositivos de RAC o grupos de dispositivos de RAC. Si el sistema ejecuta

el modo de Windows 2000 o superior, use grupos universales para expandir dominios con el usuario o los objetos de RAC.

Es posible agregar grupos de usuarios y dispositivos de RAC.

Adición de usuarios o grupos de usuarios

Para agregar usuarios o grupos de usuarios:

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

Adición de privilegios

Para agregar privilegios:

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

   Haga clic en la ficha **Objeto de privilegio** para agregar el objeto de privilegio a la asociación que define los privilegios del usuario o del grupo de usuarios al autentificar un dispositivo de RAC. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

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

Para agregar dispositivos de RAC o grupos de dispositivos de RAC:

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Introduzca el nombre de los dispositivos de RAC o de los grupos de dispositivos de RAC y haga clic en **Aceptar**.
3. En la ventana **Propiedades**, haga clic en **Aplicar** y en **Aceptar**.

   Haga clic en la ficha **Productos** para agregar uno o varios dispositivos de RAC a la asociación. Los dispositivos asociados especifican los dispositivos de RAC conectados a la red que están disponibles para los usuarios o grupos de usuarios definidos. Se pueden agregar varios dispositivos de RAC a un objeto de asociación.

Configuración de Active Directory con esquema extendido mediante la interfaz web del CMC

Para configurar Active Directory con esquema extendido mediante la interfaz web del CMC:

NOTA: Para obtener información acerca de los distintos campos, consulte la *Online Help*.

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Autenticación del usuario → Descripción general del chasis → Servicios Directory**.
2. Seleccione **Microsoft Active Directory (esquema extendido)**.

   Las opciones a configurar para el esquema extendido aparecerán en la misma página.
3. En la sección **Valores comunes**, especifique lo siguiente:
   - Seleccione **Activar Active Directory** e introduzca el valor de tiempo de espera para Active Directory en el campo **Tiempo de espera de AD** .
   - Para obtener las controladoras de dominio de Active Directory de una búsqueda en el DNS, seleccione **Buscar controladoras de dominio con DNS** y, a continuación, seleccione una de las opciones siguientes:

- **Dominio de usuario desde inicio de sesión**: para realizar una búsqueda en el DNS con el nombre de dominio del usuario de inicio de sesión.
- **Especificar un dominio**: introduzca el nombre del dominio para utilizar en la búsqueda en el DNS.

• Para activar el CMC y utilizar las direcciones del servidor de la controladora de dominio de Active Directory especificadas, seleccione **Especificar direcciones de la controladora de dominio** . Estas son las direcciones de las controladoras de dominio donde se ubican el objeto de dispositivo del CMC y los objetos asociados.

4. Haga clic en **Aplicar** para guardar la configuración.

   NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.

5. En la sección **Configuración del esquema extendido**, escriba el nombre del dispositivo de CMC y el nombre de dominio.
6. Si ha activado la validación de certificados, debe cargar en el CMC el certificado firmado por una autoridad de certificados raíz para el bosque de dominio. En la sección **Administrar certificados**, escriba la ruta de acceso del archivo o busque el archivo de certificado. Haga clic en **Cargar** para cargar el archivo en el CMC.

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

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

   PRECAUCIÓN: La validación de certificados SSL se requiere de forma predeterminada. No se recomienda desactivar este certificado.
7. Si ha activado el inicio de sesión único (SSO), en la sección Archivo keytab de Kerberos, haga clic en **Examinar**, especifique el archivo keytab y haga clic en **Cargar**. Una vez completada la carga, se mostrará un mensaje donde se indicará si la carga se ha realizado correctamente o ha fallado.
8. Haga clic en **Apply (Aplicar)**.

   El servidor web del CMC se reiniciará automáticamente al hacer clic en **Aplicar**.
9. Inicie sesión en la interfaz web del CMC.
10. En el árbol del sistema, seleccione **Chasis**, haga clic en la ficha **Red** y seleccione la subficha **Red**. Aparecerá la página **Configuración de la red**.
11. Si la opción **Usar DHCP** para la dirección IP de la interfaz de red del CMC está activada, realice una de las siguientes operaciones:
    - Seleccione la opción **Usar DHCP para obtener direcciones de servidor DNS** a fin de permitir que el servidor DHCP obtenga las direcciones del servidor DNS automáticamente.
    - Configure manualmente una dirección IP de servidor DNS. Para eso, desactive la casilla **Usar DHCP para obtener direcciones de servidor DNS** y escriba las direcciones IP de los servidores DNS primario y alternativo en los campos correspondientes.
12. Haga clic en **Aplicar cambios**.

    Se habrán configurado las opciones de Active Directory para el esquema extendido.

Configuración de Active Directory con esquema extendido mediante RACADM

Para configurar Active Directory de CMC con esquema extendido mediante los comandos RACADM, abra el símbolo del sistema e introduzca los siguientes comandos en el símbolo del sistema:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o
```

```
cfgADRacName <RAC common name> racadm config -g cfgActiveDirectory -o
cfgADRacDomain < fully qualified rac domain name > racadm config -g
cfgActiveDirectory -o cfgADDomainController1 < fully qualified domain name or
IP Address of the domain controller > racadm config -g cfgActiveDirectory -o
cfgADDomainController2 < fully qualified domain name or IP Address of the
domain controller > racadm config -g cfgActiveDirectory -o
cfgADDomainController3 < fully qualified domain name or IP Address of the
domain controller >
```

NOTA: Debe configurar al menos una de las tres direcciones. CMC intenta conectarse a cada una de las direcciones configuradas una a la vez hasta que establezca correctamente una conexión. Con el esquema extendido, estas son las direcciones FQDN o IP de las controladoras de dominio donde se encuentra este dispositivo CMC.

Para desactivar la validación de certificado durante el protocolo de enlace (opcional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

NOTA: En este caso, no tiene que cargar un certificado de CA.

Para aplicar la validación de certificado durante el protocolo de enlace SSL (opcional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

En este caso, debe cargar un certificado de CA.

```
racadm sslcertupload -t 0x2 -f < ADS root CA certificate >
```

NOTA: Si está activada la validación de certificados, especifique las direcciones de servidor de controladora de dominio y el FQDN. Asegúrese de que el DNS está configurado correctamente.

El siguiente comando de RACADM es opcional:

```
racadm sslcertdownload -t 0x1 -f < RAC SSL certificate >
```

Configuración de los usuarios LDAP genéricos

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

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

Para activar el usuario LDAP de modo que tenga acceso a una tarjeta específica del CMC, el nombre del grupo de funciones y su nombre de dominio se deben configurar en la tarjeta específica del CMC. Es posible configurar cinco grupos de funciones como máximo en cada CMC. Existe la opción de agregar un usuario a varios grupos dentro del servicio de directorio. Si un usuario es miembro de varios grupos, el usuario obtiene los privilegios de todos sus grupos.

Para obtener información sobre el nivel de privilegios de los grupos de funciones y los valores predeterminados de esos grupos, consulte Tipos de usuarios.

Configuración del directorio LDAP genérico para acceder a CMC

La implementación de LDAP genérico del CMC utiliza dos fases para otorgar acceso a la autentificación usuario-usuario y a la autorización de usuarios.

Autentificación de usuarios LDAP

Algunos servidores de directorio requieren un enlace antes de que pueda buscarse un servidor LDAP específico.

Para autentificar un usuario:

1. De forma opcional, establezca un enlace con el servicio de directorio. El enlace predeterminado es anónimo.
2. Busque el usuario según el nombre de inicio de sesión del usuario. El atributo predeterminado es `uid`. Si se encuentra más de un objeto, el proceso mostrará un mensaje de error.
3. Desenlazar y enlazar con el nombre de dominio y la contraseña del usuario. Si el sistema no puede enlazar, el inicio de sesión no será posible.
4. Si estos pasos se completan correctamente, el usuario se considera autentificado.

Autorización de usuarios LDAP

Para autorizar un usuario:

1. Busque dentro de cada grupo configurado el nombre de dominio del usuario dentro de los atributos de `member or uniqueMember`. Un administrador puede configurar el dominio de un usuario.
2. Otórguele al usuario derechos y privilegios de acceso adecuados para cada grupo de usuarios al que este pertenece.

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web del CMC

Para configurar el servicio de directorio LDAP genérico:

NOTA: Es necesario contar con el privilegio de **Administrador de configuración del chasis**.

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Autentificación de usuario** → **Servicios de directorio**.
2. Seleccione **LDAP genérico**.

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

   NOTA: Para obtener información acerca de los distintos campos, consulte la *Online Help*.

   - Configuración común
   - Servidor que se debe usar con LDAP:
     - Servidor estático: especifique la dirección IP o el nombre de dominio completo y el número de puerto LDAP.
     - Servidor DNS: especifique el servidor DNS para recuperar una lista de los servidores LDAP. Para eso, busque el registro de SRV dentro de DNS.

       Se ejecutará la siguiente consulta de DNS para los registros de SRV:

       `_[Service Name]._tcp.[Search Domain]`

donde <*Search Domain*> es el dominio de nivel raíz que se utiliza en la consulta y <*Service Name*> indica el nombre del servicio que se debe utilizar en la consulta.

Por ejemplo:

`_ldap._tcp.dell.com`

donde `ldap` es el nombre del servicio y `dell.com` es el dominio de búsqueda.

4. Haga clic en **Aplicar** para guardar la configuración.

   NOTA: Es necesario aplicar los valores de configuración antes de continuar. Si no se aplican los valores, la configuración se pierde al desplazarse a la siguiente página.

5. En la sección **Configuración de grupo**, haga clic en un **Grupo de funciones**.
6. En la página **Configurar grupo de funciones de LDAP**, especifique los privilegios y el nombre del dominio del grupo para el grupo de funciones.
7. Haga clic en **Aplicar** para guardar la configuración del grupo de funciones, haga clic en **Volver a la página de configuración** y seleccione **LDAP genérico**.
8. Si ha seleccionado la opción **Validación de certificado activada**, en la sección **Administrar certificados**, especifique el certificado de CA para validar el certificado de servidor LDAP durante un protocolo de enlace SSL y haga clic en **Cargar**. El certificado se cargará al CMC y se mostrarán los detalles.
9. Haga clic en **Apply (Aplicar)**.

   Se configura el servicio de directorio LDAP.

Configuración del servicio de directorio LDAP genérico mediante RACADM

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

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

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

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

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

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

`_ldap._tcp.domainname.com`

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

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

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

de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en **dell.com/support/manuals**.

10

Configuración del CMC para inicio de sesión único o inicio de sesión mediante tarjeta inteligente

En esta sección se proporciona información para configurar el CMC para el inicio de sesión único (SSO) y el inicio de sesión mediante tarjeta inteligente en los usuarios de Active Directory.

El inicio de sesión único utiliza Kerberos como método de autentificación, lo que permite que los usuarios que han iniciado sesión en el dominio realicen un inicio de sesión único o automático a las aplicaciones subsiguientes como Exchange. Para el inicio de sesión único, el CMC utiliza las credenciales del sistema cliente que el sistema operativo almacena en caché después de que el usuario inicia sesión mediante una cuenta de Active Directory válida.

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

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

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 y Windows Server 2008 pueden usar Kerberos como el mecanismo de autentificación para el inicio de sesión único y el inicio de sesión mediante tarjeta inteligente.

Para obtener información sobre Kerberos, consulte el sitio web de Microsoft.

Requisitos del sistema

Para utilizar la autentificación de Kerberos, la red debe incluir:

- Servidor DNS
- Servidor de Microsoft Active Directory

NOTA: Si usa Active Directory en Windows 2003, asegúrese de tener las revisiones y los Service Pack más recientes instalados en el sistema cliente. Si usa Active Directory en Windows 2008, asegúrese de tener instalado SP1 junto con las siguientes correcciones urgentes:

Windows6.0-KB951191-x86.msu para la utilidad KTPASS. Sin esta revisión, la utilidad genera archivos keytab dañados.

Windows6.0-KB957072-x86.msu para utilizar transacciones GSS_API y SSL durante un enlace de LDAP.

- Centro de distribución de claves Kerberos (se incluye con el software de servidor Active Directory).
- Servidor DHCP (recomendado).
- La zona inversa del servidor DNS debe tener una entrada para el servidor Active Directory y el CMC.

Sistemas cliente

- Solamente para el inicio de sesión mediante tarjeta inteligente, el sistema cliente debe tener el paquete redistribuible Microsoft Visual C++ 2005. Para obtener más información, consulte **www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**.
- Para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente, el sistema cliente debe formar parte del dominio de Active Directory y del territorio de Kerberos.

CMC

- Cada CMC debe tener una cuenta de Active Directory.
- El CMC debe formar parte del dominio de Active Directory y del territorio de Kerberos.

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

A continuación se indican los prerrequisitos para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente:

- Configure el territorio de Kerberos y el centro de distribución de claves (KDC) para Active Directory (ksetup).
- Una sólida infraestructura de NTP y DNS para evitar problemas de desfase de tiempo y búsqueda inversa.
- Configure el CMC y el grupo de funciones de esquema estándar de Active Directory con miembros autorizados.
- Para la tarjeta inteligente, cree usuarios de Active Directory para cada CMC, configurados para utilizar el cifrado DES de Kerberos pero no la preautentificación.
- Configure el explorador para el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente.
- Registre a los usuarios de CMC en el centro de distribución de claves con Ktpass (esto también genera una clave que se carga en el CMC).

Generación del archivo Keytab de Kerberos

Para admitir la autentificación de inicio de sesión único y de inicio de sesión mediante tarjeta inteligente, el CMC admite la red Kerberos de Windows. La herramienta ktpass (disponible en Microsoft como parte de los CD/DVD de instalación de servidores) se utiliza para crear enlaces de nombre principal de servicio (SPN) a una cuenta de usuario y exportar la información de confianza a un archivo keytab de Kerberos de estilo MIT. Para obtener más información sobre la utilidad ktpass, consulte el sitio web de Microsoft.

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

Para generar un archivo keytab mediante la herramienta ktpass:

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

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

   NOTA: Según los requisitos de RFC, el elemento `cmcname.domainname.com` se debe escribir en minúscula y `@REALM_NAME` en mayúscula. Además, CMC admite el tipo de criptografía DES-CBC-MD5 para la autentificación de Kerberos.

   Se generará un archivo keytab que se debe cargar en el CMC.

   NOTA: El archivo keytab contiene una clave de cifrado y debe conservarse en un lugar seguro. Para obtener más información sobre la utilidad *ktpass*, consulte el sitio web de **Microsoft**.

Configuración del CMC para el esquema de Active Directory

Para obtener información sobre la forma de configurar el CMC para el esquema estándar de Active Directory, consulte Configuración del esquema estándar de Active Directory.

Para obtener información sobre la forma de configurar el CMC para el esquema extendido de Active Directory, consulte Descripción general del esquema extendido de Active Directory.

Configuración del explorador para el inicio de sesión único

El inicio de sesión único (SSO) es compatible con Internet Explorer versiones 6.0 y superiores, y Firefox versiones 3.0 y superiores.

NOTA: Las instrucciones siguientes se aplican solamente si el CMC utiliza el inicio de sesión único con la autentificación de Kerberos.

Internet Explorer

Para configurar Internet Explorer para inicio de sesión único:

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

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

   Se muestra el cuadro de diálogo **Configuración avanzada de Intranet local**.

5. En el campo **Agregar este sitio a la zona**, escriba el nombre del CMC y el dominio al cual pertenece y haga clic en **Agregar**.

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

Mozilla Firefox

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

   NOTA: Si el explorador muestra la advertencia **Esto puede anular su garantía**, haga clic en **Seré cuidadoso, lo prometo**.
2. En el cuadro de texto **Filtro**, escriba **negotiate**.

   El explorador muestra una lista de nombres preferidos limitada a aquéllos que contienen la palabra "negotiate".
3. En la lista, haga doble clic en **network.negotiate-auth.trusted-uris**.
4. En el cuadro de diálogo **Ingresar valor de la cadena**, escriba el nombre de dominio del CMC y haga clic en **Aceptar**.

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

Internet Explorer: asegúrese de que el explorador de Internet esté configurado para descargar los complementos Active-X.

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

Es posible usar la interfaz web del CMC o RACADM para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente en el CMC.

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

Para configurar el inicio de sesión único o el inicio de sesión mediante tarjeta inteligente de Active Directory en el CMC:

NOTA: Para obtener más información acerca de estas opciones, consulte *Online Help*.

1. Mientras configura Active Directory, para establecer una cuenta de usuario, realice los siguientes pasos adicionales:
   - Cargue el archivo keytab.
   - Para activar el inicio de sesión único, seleccione la opción **Activar inicio de sesión único**.
   - Para activar el inicio de sesión mediante tarjeta inteligente, seleccione la opción **Activar inicio de sesión mediante tarjeta inteligente**.

NOTA: Si estas dos opciones están seleccionadas, todas las interfaces fuera de banda de línea de comandos, incluida secure shell (SSH), Telnet, serie y RACADM remoto permanecen sin cambios.

2. Haga clic en **Aplicar**.

   La configuración se guarda.

   Es posible probar Active Directory con la autentificación de Kerberos mediante el comando de RACADM:

   ```
   testfeature -f adkrb -u <user>@<domain>
   ```

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

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

Carga de un archivo keytab

El archivo keytab de Kerberos sirve como credencial de nombre de usuario y contraseña del CMC para el centro de datos de Kerberos (KDC), que a su vez autoriza el acceso a Active Directory. Cada CMC dentro del territorio de Kerberos se debe registrar con Active Directory y debe tener un archivo keytab exclusivo.

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

Para cargar el archivo keytab:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Autentificación de usuario → Servicios de directorio**.
2. Seleccione **Microsoft Active Directory (Esquema estándar)**.
3. En la sección **Archivo keytab de Kerberos**, haga clic en **Examinar**, seleccione el archivo keytab y haga clic en **Cargar**.

   Una vez completada la carga, se mostrará un mensaje donde se indicará si el archivo keytab se ha cargado correctamente o no.

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

Además de los pasos que se realizan durante la configuración de Active Directory, ejecute el siguiente comando para activar el inicio de sesión único:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

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

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

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

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

Funciones de la consola de línea de comandos del CMC

El CMC admite las siguientes funciones de consola serie, Telnet y SSH:

- Una conexión de cliente serie y hasta cuatro conexiones simultáneas de cliente Telnet.
- Hasta cuatro conexiones simultáneas de cliente Secure Shell (SSH).
- Compatibilidad para comandos RACADM.
- Comando de conexión integrado que se conecta a la consola serie de servidores y a los módulos de E/S; también disponible como `racadm connect`.
- Historial y edición de línea de comandos.
- Control del tiempo de espera de las sesiones en todas las interfaces de consola.

Comandos para la interfaz de la línea de comandos del CMC

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

Tabla 22. Comandos para la línea de comandos del CMC

Comando	Descripción
`racadm`	Los comandos RACADM empiezan con la palabra clave `racadm` seguida de un subcomando. Para obtener más información, consulte la *Guía de referencia sobre la línea de comando RACADM de Chassis Management Controller para PowerEdge VRTX*.
`connect`	Establece una conexión a la consola serie de un servidor o módulo de E/S. Para obtener más información, consulte Conexión a servidores o módulos de E/S mediante el comando connect.

Comando	Descripción
	NOTA: También se puede usar el comando RACADM `connect`.
`exit`, `logout` y `quit`	Todos estos comandos ejecutan la misma acción. Terminan la sesión actual y regresan a una interfaz de línea de comandos de inicio de sesión.

Uso de una consola Telnet con el CMC

Es posible mantener hasta cuatro sesiones Telnet con el CMC de forma simultánea.

Si Management Station ejecuta Windows XP o Microsoft Windows Server 2003, es posible que tenga un problema con los caracteres en las sesiones Telnet del CMC. Este problema puede presentarse como un bloqueo de la pantalla de inicio de sesión en el que la tecla Entrar no responde y no aparece la petición de contraseña.

Para reparar este problema, descargue la revisión hotfix 824810 en **support.microsoft.com**. Para obtener más información, también puede consultar el artículo 824810 de Microsoft Knowledge Base.

Uso de SSH con el CMC

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

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

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

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

Se admiten cuatro sesiones SSH simultáneas por vez. El tiempo de espera de la sesión es controlado por la propiedad `cfgSsnMgtSshIdleTimeout`. Para obtener más información sobre los comandos RACADM, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en dell.com/support/Manuals.

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

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

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

Esquemas de criptografía SSH compatibles

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

Tabla 23. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS de 512–1024 bits (aleatorio) según la especificación NIST
Criptografía simétrica	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Integridad del mensaje	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Autentificación	Contraseña

Configuración de la autentificación de clave pública en SSH

Es posible configurar hasta 6 claves públicas que se pueden utilizar con el nombre de usuario service en la interfaz de SSH. Antes de agregar o eliminar claves públicas, asegúrese de utilizar el comando `view` para ver las claves que ya están configuradas y no sobrescribir ni eliminar accidentalmente una clave. El nombre de usuario service es una cuenta de usuario especial que se puede utilizar para acceder al CMC mediante SSH. Cuando la autentificación de clave pública en SSH se configura y se utiliza correctamente, no es necesario introducir un nombre de usuario ni una contraseña para iniciar sesión en el CMC. Esta función puede resultar de gran utilidad para configurar secuencias de comandos automáticas para ejecutar diversas funciones.

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

Al agregar claves públicas nuevas, asegúrese de que las claves existentes no se encuentren ya en el índice donde desea agregar la clave nueva. El CMC no realiza comprobaciones para verificar que las claves anteriores se hayan eliminado antes de agregar una nueva. Tan pronto como se agrega una clave nueva, esa clave entra en vigor automáticamente siempre y cuando la interfaz de SSH esté activada.

Cuando utilice la sección de comentario de la clave pública, recuerde que el CMC solo utiliza los primeros 16 caracteres. El CMC utiliza el comentario de la clave pública para distinguir a los usuarios de SSH cuando utilizan el comando `getssninfo` de RACADM, ya que todos los usuarios de autentificación de clave pública usan el nombre de usuario service para iniciar sesión.

Por ejemplo, si se configuran dos claves públicas, una con el comentario PC1 y otra con el PC2:

```
racadm getssninfo Tipo Usuario Dirección IP Fecha y hora de conexión SSH PC1
x.x.x.x 06/16/2009 09:00:00 SSH PC2 x.x.x.x 06/16/2009 09:00:00
```

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

Generación de claves públicas para sistemas que ejecutan Windows

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

En esta sección se describen instrucciones sencillas para generar un par de claves pública-privada en ambas aplicaciones. Para ver usos adicionales o avanzados de estas herramientas, consulte la ayuda de la aplicación.

Para usar el Generador de claves PuTTY a fin de crear una clave básica para clientes que ejecutan Windows:

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

   NOTA:
   - La longitud de la clave DSA recomendada es de 1024.
   - Es posible que el CMC no muestre un mensaje si se agregan claves menores de 768 o mayores de 4096, pero el CMC deja de responder al intentar iniciar sesión con esas claves.
   - Para las claves DAS mayores de 2048, use el siguiente comando RACADM. El CMC acepta las claves RSA hasta la clave 4096, pero la fortaleza recomendada de la clave es 1024.

     ```
     racadm -r 192.168.8.14 -u root -p calvin sshpkauth -i svcacct -k 1 -p
     0xfff -f dsa_2048.pub
     ```
3. Haga clic en **Generar** y mueva el mouse dentro de la ventana como se indica.

   Después de crear la clave, se puede modificar el campo de comentario de la clave.

   También se puede especificar una frase de contraseña para proteger la clave. Asegúrese de guardar la clave privada.
4. Hay dos opciones para utilizar la clave pública:
   - Guardar la clave pública en un archivo para cargarlo más tarde.
   - Copiar y pegar el texto de la ventana **Clave pública para pegar** al agregar la cuenta mediante la opción de texto.

Generación de claves públicas para sistemas que ejecutan Linux

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

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

donde:

`-t` debe ser dsa o rsa.

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

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

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

Notas de la sintaxis de RACADM para CMC

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

- Para la opción `-i`, el parámetro debe ser `svcacct`. Todos los demás parámetros para `-i` fallan en el CMC. `svcacct` es una cuenta especial para la autentificación de clave pública sobre SSH en el CMC.
- Para iniciar sesión en el CMC, el usuario debe ser service. Los usuarios de otras categorías tienen acceso a las claves públicas introducidas mediante el comando `sshpkauth`.

Visualización de claves públicas

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

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

Para ver una clave a la vez, reemplace `all` por un número de 1 a 6. Por ejemplo, para ver la clave 2, escriba:

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

Adición de claves públicas

Para agregar una clave pública al CMC mediante la opción de carga de archivos `-f`, en la consola de la interfaz de la línea de comandos, escriba:

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

NOTA: Solo puede usar la opción de carga de archivos con RACADM remoto. Para obtener información, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia sobre la línea de comando RACADM de Chassis Management Controller para PowerEdge VRTX).

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

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

Eliminación de claves públicas

Para eliminar una clave pública, ejecute el siguiente comando:

```
racadm sshpkauth -i svcacct -k 1 -d
```

Para eliminar todas las claves públicas, ejecute el siguiente comando:

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

Configuración del software de emulación de terminal

El CMC admite una consola de texto en serie de una estación de administración que ejecuta uno de los siguientes tipos de software de emulación de terminal:

- Minicom de Linux.
- HyperTerminal Private Edition (versión 6.3) de Hilgraeve.

Ejecute las tareas en las subsecciones siguientes para configurar el tipo de software de terminal necesario.

Configuración de Minicom de Linux

Minicom is una utilidad de acceso de puerto serie para Linux. Los siguientes pasos son válidos para configurar Minicom versión 2.0. Es posible que otras versiones de Minicom difieran un poco, pero requieren la misma configuración básica. Para configurar otras versiones de Minicom, consulte la información en la sección Configuración requerida de Minicom de esta Guía del usuario.

Configuración de Minicom versión 2.0

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

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

1. Si no tiene el archivo de configuración de Minicom, vaya al siguiente paso. Si lo tiene, escriba `minicom<Minicom config file name>` y avance al paso 12.
2. En la petición de comandos de Linux, escriba `minicom –s`.
3. Seleccione **Configuración del puerto serie** y presione <Intro>.
4. Presione <a> y seleccione el dispositivo de serie correspondiente (por ejemplo, `/dev/ttyS0`).
5. Presione <e> y defina la opción **Bps/Par/Bits** con el valor **115200 8N1**.
6. Presione <f> y defina la opción **Control de flujo de hardware** en el valor **Sí** y luego defina la opción **Control de flujo de software** en el valor **No**. Para salir del menú **Configuración del puerto serie**, presione <Intro>.
7. Seleccione **Módem y marcación** y presione <Intro>.
8. En el menú **Configuración de parámetros y marcación de módem**, presione <Retroceso> para borrar los valores **init**, **reset**, **connect** y **hangup** de modo que queden en blanco; luego presione <Intro> para guardar cada valor en blanco.
9. Cuando se hayan borrado todos los campos especificados, presione <Intro> para salir del menú **Configuración de parámetros y marcación de módem**.
10. Seleccione **Salir de Minicom** y presione <Intro>.
11. En la petición de shell de comandos, escriba `minicom <Minicom config file name>`.
12. Para salir de Minicom, presione <Ctrl><a>, <x>, <Intro>.

    Asegúrese de que la ventana Minicom muestre una petición de inicio de sesión. Cuando esta aparezca, la conexión se habrá completado con éxito. Desde ese momento, podrá iniciar sesión y obtener acceso a la interfaz de línea de comandos de CMC.

Valores de Minicom necesarios

Consulte la siguiente tabla para configurar cualquier versión de Minicom.

Tabla 24. Configuración de Minicom

Descripción del valor	Valor necesario
Bps/Par/Bits	115200 8N1
Control de flujo de hardware	Sí

Descripción del valor	Valor necesario
Control de flujo de software	No
Emulación de terminal	ANSI
Configuración de parámetros y marcación de módem	Borre los valores **init**, **reset**, **connect** y **hangup** de modo que queden en blanco.

Conexión a servidores o módulos de E/S con el comando connect

El CMC puede establecer una conexión para redirigir la consola serie del servidor o los módulos de E/S.

Para los servidores, la redirección de consola serie se puede llevar a cabo mediante:

- la interfaz de línea de comandos del CMC (CLI) o el comando RACADM `connect`. Para obtener más información sobre cómo ejecutar los comandos RACADM, consulte la *Guía de referencia sobre línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX*.
- La función de redirección de consola serie de la interfaz web del iDRAC.
- La función de comunicación en serie en la LAN (SOL) del iDRAC.

En una consola serie, Telnet o SSH, el CMC admite el comando `connect` para que establezca una conexión serie con un servidor o un módulo de E/S. La consola de servidor serie contiene las pantallas de configuración e inicio del BIOS, así como la consola serie del sistema operativo. En el caso del módulo de E/S, hay disponible una consola serie de conmutación. En el chasis hay un solo módulo de E/S.

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 para la seguridad.

NOTA: El comando `connect` ofrece la opción `–b` (binario). La opción `–b` transmite datos binarios sin procesar y no utiliza `cfgSerialConsoleQuitKey`. Además, al establecer conexión con un servidor por medio de la consola serie del CMC, las transiciones en la señal DTR (por ejemplo, si se quita el cable serie para conectar un depurador) no causan una desconexión de la aplicación.

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

Para conectarse a un módulo de E/S escriba:

`connect switch-`*`n`*

en donde `n` es un módulo de E/S con la etiqueta A1.

Cuando se hace referencia al módulo de E/S en el comando connect, el módulo se asigna a un conmutador como muestra la siguiente tabla.

Tabla 25. Asignación de módulos de E/S en conmutadores

Etiqueta del módulo de E/S	Conmutador
A1	switch-a1 o switch- 1

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

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

Para conectarse a una consola serie administrada por el servidor, ejecute el comando `connect server-n`, en donde *n* es un valor del 1 al 4. También pude usar el comando `racadm connect server-n`. Al conectarse a un servidor mediante la opción `-b`, se asume una comunicación binaria y se desactiva el carácter de escape. Si el iDRAC no está disponible, aparecerá el mensaje de error `No route to host`.

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

NOTA: Para ver las pantallas de inicio del BIOS, la redirección serie tiene que estar activada en la configuración de BIOS del servidor. Además, se debe configurar la pantalla del emulador terminal en 80x25. De lo contrario, los caracteres de la página no se mostrarán correctamente.

NOTA: No todas las teclas funcionan en las páginas de configuración del BIOS. Por lo tanto, defina los atajos de teclado correctos para <Ctrl> <Alt> <Supr> y otras funciones. La pantalla de redirección inicial muestra los atajos necesarios.

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

Puede usar una sesión de consola remota para conectarse al sistema administrado mediante la interfaz web del iDRAC (consulte la *iDRAC User's Guide* (Guía del usuario de iDRAC) en **dell.com/support/manuals**).

La comunicación 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. Encienda el servidor administrado.
2. Presione <F2> para acceder a la utilidad de configuración del BIOS durante la autoprueba de encendido.
3. Vaya a **Comunicación en serie** y presione <Intro> . En el cuadro de diálogo, la lista de comunicación en serie muestra las siguientes opciones:
   - **desactivado**
   - **Encendido sin redirección de consola**
   - **Encendido con redirección de consola a través de COM1**

   Para navegar entre estas opciones, presione las teclas de flechas correspondientes.

   NOTA: Asegúrese de seleccionar la opción **Encendido con redirección de consola a través de COM1**.
4. Active **Redirección después del inicio** (el valor predeterminado está **desactivado**). Esta opción permite la redirección de consola del BIOS en inicios posteriores.
5. Guarde los cambios y salga.

   El sistema administrado se reiniciará.

Configuración de Windows para la redirección de consola en serie

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

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

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

NOTA: Al configurar la ventana de emulación del cliente VT100, defina la ventana o aplicación que muestra la consola redirigida en 25 filas por 80 columnas para garantizar que se muestre el texto correctamente. De lo contrario, algunas pantallas de texto pueden aparecer distorsionadas.

Modifique el archivo **/etc/grub.conf** según se indica a continuación:

1. Localice las secciones de configuración general en el archivo y agregue las siguientes dos líneas nuevas:

   ```
   serial --unit=1 --speed=57600 terminal --timeout=10 serial
   ```

2. Anexe dos opciones a la línea de núcleo:

   ```
   consola de núcleo=ttyS1,57600
   ```

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

   El siguiente ejemplo ilustra los cambios descritos en este procedimiento.

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

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

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

     ```
     consola=ttyS1,57600
     ```

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

Configuración de Linux para la redirección de consola serie del servidor después del inicio

Edite el archivo **/etc/inittab**, como se indica a continuación:

Agregue una nueva línea para configurar `agetty` en el puerto serie COM2:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

El siguiente ejemplo muestra el archivo con la nueva línea.

```
# # inittab This file describes how the INIT process # should set up the system
in a certain # run-level. # # Author: Miquel van Smoorenburg # Modified for RHS
Linux by Marc Ewing and # Donnie Barnes # # Default runlevel. The runlevels
used by RHS are: # 0 - halt (Do NOT set initdefault to this) # 1 - Single user
mode # 2 - Multiuser, without NFS (The same as 3, if you # do not have
networking) # 3 - Full multiuser mode # 4 - unused # 5 - X11 # 6 - reboot (Do
NOT set initdefault to this) # id:3:initdefault: # System initialization.
si::sysinit:/etc/rc.d/rc.sysinit l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/
rc.d/rc 1 l2:2:wait:/etc/rc.d/rc 2 l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/
rc.d/rc 4 l5:5:wait:/etc/rc.d/rc 5 l6:6:wait:/etc/rc.d/rc 6 # Things to run in
every runlevel. ud::once:/sbin/update # Trap CTRL-ALT-DELETE ca::ctrlaltdel:/
sbin/shutdown -t3 -r now # When our UPS tells us power has failed, assume we
have a few # minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your # UPS is
connected and working correctly. pf::powerfail:/sbin/shutdown -f -h +2 "Power
Failure; System Shutting Down" # If power was restored before the shutdown
kicked in, cancel it. pr:12345:powerokwait:/sbin/shutdown -c "Power Restored;
Shutdown Cancelled" # Run gettys in standard runlevels co:2345:respawn:/sbin/agetty -
h -L 57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/
mingetty tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty
tty4 5:2345:respawn:/sbin/mingetty tty5 6:2345:respawn:/sbin/mingetty tty6 #
Run xdm in runlevel 5 # xdm is now a separate service x:5:respawn:/etc/X11/
prefdm -nodaemon
```

Edite el archivo **/etc/securetty** de la siguiente manera:

Agregue una nueva línea, con el nombre del tty serie para COM2:

```
ttyS1
```

El siguiente ejemplo muestra un archivo con la nueva línea.

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4
tty5 tty6 tty7 tty8 tty9 tty10 tty11 ttyS1
```

12

Uso de las tarjetas FlexAddress y FlexAddress Plus

Esta sección proporciona información acerca de las tarjetas FlexAddress, FlexAddress Plus y sobre cómo configurar y usar estas tarjetas.

NOTA: Se debe instalar una licencia Enterprise en el CMC para poder utilizar la función FlexAddress.

Acerca de FlexAddress

Si se reemplaza un servidor, la función FlexAddress de la ranura sigue siendo igual para la ranura del servidor dado. Si el servidor se inserta en una nueva ranura o un nuevo chasis, se utiliza la dirección WWN/MAC asignada por el servidor, a menos que el chasis particular tenga la función FlexAddress activada para la ranura nueva. Si quita el servidor, regresará a la dirección asignada por el servidor. No es necesario volver a configurar los marcos de implementación, los servidores DHCP y los enrutadores de diversas redes Fabric para identificar el servidor nuevo.

A cada módulo del servidor se le asignan direcciones WWN y/o MAC exclusivas como parte del proceso de fabricación. Sin FlexAddress, si tiene que reemplazarse un servidor con otro módulo de servidor, las direcciones WWN/MAC cambian y las herramientas de administración de red Ethernet y los recursos SAN tienen que volver a configurarse para identificar el nuevo módulo del servidor.

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

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

El chasis VRTX del CMC se envía con la tarjeta SD, que admite las funciones FlexAddress, FlexAddress Plus y almacenamiento extendido. Si el chasis VRTX se suministra con un segundo CMC opcional, el segundo CMC tiene una tarjeta SD que únicamente admite el almacenamiento extendido.

NOTA:

- La información contenida en la tarjeta SD está cifrada y no es posible duplicarla o alterarla de ninguna forma porque podría desactivar las funciones del sistema y ocasionar que el sistema deje de funcionar.
- El uso de una tarjeta SD se limita a un solo chasis. No puede utilizar la misma tarjeta SD en otro chasis.

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

```
<mac_start> + <mac_count> - 1 = <mac_end>
```

Por ejemplo:

```
(starting_mac)00188BFFDCFA + (mac_count)0xCF - 1 = (ending_mac)00188BFFDDC8
```

.

NOTA: Bloquee la tarjeta SD antes de insertarla en el lector de tarjetas de memoria USB para evitar modificar accidentalmente el contenido. Debe desbloquear la tarjeta SD antes de insertarla en el CMC.

Acerca de FlexAddress Plus

FlexAddress Plus es una nueva función que se agrega a la versión 2.0 de la tarjeta de función. Se trata de una actualización de la tarjeta de función FlexAddress versión 1.0. La función FlexAddressPlus contiene más direcciones MAC que FlexAddress. Ambas funciones permiten que el chasis asigne direcciones WWN/MAC (Nombre mundial/Control de acceso de medios) a dispositivos Fibre Channel y Ethernet. Las direcciones WWN/MAC asignadas por el chasis son únicas a nivel mundial y específicas para una ranura de servidor.

Visualización del estado de activación de FlexAddress

Una tarjeta de función que contiene una o más de las siguientes funciones: FlexAddress, FlexAddress Plus y/o almacenamiento extendido.

Para ver el estado de FlexAddress del chasis mediante la interfaz web del CMC, vaya a **Descripción general del chasis → Configuración**.

Aparecerá la página **Configuración general del chasis**.

FlexAddress tiene un valor **Activo** o **No activo**. El valor **Activo** indica que la función está instalada en el chasis, mientras que **No activo** indica que la función no está instalada y no está en uso en el chasis.

Ejecute el siguiente comando de RACADM para ver el estado de la tarjeta de función SD:

```
racadm featurecard -s
```

Aparece el mensaje siguiente:

```
Active CMC: The feature card inserted is valid, serial number
CN0H871T1374036T00MXA00 The feature card contains the following feature(s)
FlexAddress: bound FlexAddressPlus: bound ExtendedStorage: bound Standby CMC:
The feature card contains the following feature(s) ExtendedStorage: bound
```

NOTA: El CMC secundario es opcional y el resultado para el CMC en espera se muestra solamente si el CMC en espera está disponible en el chasis.

Tabla 26. Mensajes de estado que muestra el comando featurecard -s

Mensaje de estado	Acciones
`No feature card inserted.`	Revise el CMC para verificar que la tarjeta SD se haya insertado correctamente. En una configuración redundante del CMC, asegúrese de que el CMC con la tarjeta de función SD instalada sea el CMC activo y no el CMC en espera.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound.`	No es necesario realizar ninguna acción.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.`	Retire la tarjeta SD; coloque e instale la tarjeta SD en el chasis actual.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.`	La tarjeta de función se puede llevar a otro chasis o se puede reactivar en el chasis actual. Para reactivarla en el chasis actual, introduzca `racadm racreset` hasta que el módulo del CMC con la tarjeta de función instalada se active.

Use el siguiente comando de RACADM para mostrar todas las funciones activadas en el chasis:

```
racadm feature -s
```

El comando produce el mensaje de estado siguiente:

```
Feature Name = FlexAddress Date/time Activated = 05 Oct 2013 - 11:50:49 Feature
installed from SD-card serial number = CN0H871T1374036T00MXA00 Feature Name =
FlexAddressPlus Date/time Activated = 05 Oct 2013 - 11:50:49 Feature installed
from SD-card serial number = CN0H871T1374036T00MXA00 Feature Name =
ExtendedStorage Current Status = redundant, active Date/time Activated = 05 Oct
2013 - 11:50:58 Feature installed from SD-card serial number =
CN0H871T1374036T00MXA00
```

Si no hay funciones activas en el chasis, el comando mostrará un mensaje:

```
racadm feature -s No features active on the chassis
```

Es posible que Dell Feature Cards pueda contener más de una función. Una vez activada cualquiera de las funciones que incluye Dell Feature Card en un chasis, todas las demás funciones que se puedan incluir en Dell Feature Card no se podrán activar en un chasis diferente. En este caso, el comando `racadm feature -s` mostrará el siguiente mensaje para las funciones afectadas:

```
ERROR: One or more features on the SD card are active on another chassis
```

Para obtener más información acerca de los comandos `feature` y `featurecard`, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en el sitio de asistencia.

Desactivación de FlexAddress

Es posible desactivar la función FlexAddress y hacer que la tarjeta SD regrese a un estado previo a la instalación mediante un comando de RACADM. No hay ninguna función de desactivación en la interfaz web. La desactivación hace que la tarjeta SD regrese a su estado original, donde se la puede instalar y activar en otro chasis. El término FlexAddress, en este contexto, hace referencia tanto a FlexAddress como a FlexAddressPlus.

NOTA: La tarjeta SD debe estar instalada físicamente en el CMC y el chasis debe estar apagado antes de ejecutar el comando de desactivación.

Si ejecuta el comando de desactivación sin instalar una tarjeta SD o con una tarjeta desde un chasis diferente instalado, la función se desactiva y no se realiza el cambio en la tarjeta.

Para desactivar la función FlexAddress y restablecer la tarjeta SD:

```
racadm feature -d -c flexaddress
```

El comando muestra el siguiente mensaje de estado si se desactivó correctamente.

```
feature FlexAddress is deactivated on the chassis successfully.
```

Si el chasis no se apaga antes de ejecutar el comando, el comando muestra el siguiente error:

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

NOTA: Para activar la función FlexAddress nuevamente, instale la tarjeta de función FlexAddress en el CMC activo y reinicie el CMC.

Para obtener más información acerca del comando, consulte la sección del comando **featurae** de *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX).

Configuración de FlexAddress

FlexAddress es una actualización opcional que permite a los módulos de los servidores reemplazar la dirección WWN/MAC asignada de fábrica por una dirección WWN/MAC proporcionada por el chasis.

NOTA: En esta sección, el término FlexAddress también hace referencia a FlexAddress Plus.

NOTA: Con el subcomando `racresetcfg` puede restablecer la FlexAddress de un CMC a su configuración predeterminada de fábrica que está "desactivada". La sintaxis de RACADM es:

```
racadm racresetcfg -c flex
```

Para obtener más información sobre los comandos RACADM relacionados con FlexAddress y los datos de otras propiedades predeterminadas de fábrica, consulte la *Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX* disponible en **dell.com/support/manuals**.

El servidor debe estar apagado para iniciar la configuración. Puede activar o desactivar FlexAddress en cada red Fabric. Otra opción es activar o desactivar la función en cada ranura. Después de activarla en cada red Fabric, puede seleccionar las ranuras que activará. Por ejemplo, si se activa la red Fabric A, las ranuras activadas tendrán la función FlexAddress activada solo en la red Fabric A. Las demás redes usan la dirección WWN/MAC asignada de fábrica en el servidor.

NOTA: FlexAdress no tiene efecto en un módulo de servidor hasta el siguiente reinicio. Cuando se implementa la función FlexAddress por primera vez en un módulo del servidor, se requiere de una secuencia de apagado y encendido para que FlexAddress se active. FlexAddress en dispositivos Ethernet se programa por el BIOS del módulo del servidor. Para que el BIOS del módulo del servidor programe la dirección, necesita estar en funcionamiento, lo que requiere que el módulo del servidor se encienda. Cuando se completan las secuencias de apagado y encendido, las identificaciones MAC asignadas por el chasis están disponibles para la función de encendido en LAN (WOL).

Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis

En el nivel del chasis, puede activar o desactivar la función FlexAddress para las redes Fabric y las ranuras. FlexAddress se activa para cada red Fabric y, después, se seleccionan las ranuras que deben participar en la función. Tanto las redes Fabric como las ranuras deben activarse para configurar FlexAddress satisfactoriamente.

Configuración de FlexAddress para redes Fabric y ranuras en el nivel del chasis mediante la interfaz web del CMC

Si un servidor está presente en la ranura, apáguelo antes de activar la función FlexAddress en esa ranura.

Para activar o desactivar redes Fabric y ranuras para usar la función de FlexAddress mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del servidor** → **Configuración** → **FlexAddress**.
2. En la página **Implementar FlexAddress**, en la sección **Seleccionar redes Fabric para las direcciones WWN/MAC asignadas al chasis**, seleccione el tipo de red Fabric (**Fabric-A** o **iDRAC**) para el cual desea activar FlexAddress. Para desactivar esta función, desactive la opción.
3. En la página **Seleccionar ranuras para las direcciones WWN/MAC asignadas al chasis**, seleccione la opción **Activado** para la ranura donde desea activar FlexAddress. Para desactivar la función, desactive la opción.

   NOTA: Tenga en cuenta lo siguiente:
   - Si no se selecciona ninguna ranura, FlexAddress no se activa para la red Fabric seleccionada.
   - Si no se selecciona ninguna de las redes Fabric y se selecciona y aplica una ranura de servidor, aparece el siguiente mensaje `No fabrics selected! FlexAddress will not be used on this chassis.` Seleccione la red Fabric y la ranura para configurar FlexAddress satisfactoriamente.
   - No se permite configurar FlexAddress para una ranura esclava. La opción aparece atenuada en la interfaz web del CMC. Los dispositivos de Ethernet asociados con la ranura esclava del servidor heredan la configuración de la ranura maestra.
4. Para guardar la configuración, haga clic en **Aplicar**.

Configuración de FlexAddress para ranuras y redes Fabric en el nivel del chasis mediante RACADM

Para activar o desactivar las redes Fabric, use el siguiente comando RACADM:

```
racadm setflexaddr [-f <fabricName> <state>]
```

en donde, `<fabricName> = A or iDRAC` y `<state> = 0 or 1`

El valor 0 es desactivar y 1 es activar.

Para activar o desactivar las ranuras, use el siguiente comando RACADM:

`racadm setflexaddr [-i <slot#> <state>]`

en donde, `<slot#> = 1 o 4` y `<state> = 0 o 1`

El valor 0 es desactivar y 1 es activar.

Para obtener más información acerca del comando **setflexaddr**, consulte la *Guía de referencia sobre línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX*.

NOTA: Si adquiere la función FlexAddress o FlexAddressPlus con Dell PowerEdge VRTX, este viene preinstalado y activado para todas las ranuras y redes Fabric. Para adquirir esta función, comuníquese con Dell en dell.com.

NOTA: Con el subcomando `racresetcfg` puede restablecer la FlexAddress de un CMC a su configuración predeterminada de fábrica que está "desactivada". La sintaxis de RACADM es:

`racadm racresetcfg -c flex`

Para obtener más información sobre los comandos RACADM relacionados con FlexAddress y los datos de otras propiedades predeterminadas de fábrica, consulte la *Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX* disponible en **dell.com/support/manuals**.

Visualización de las direcciones World Wide Name/Media Access Control (WWN/MAC)

La página **Resumen de WWN/MAC** permite ver la configuración de WWN y la dirección MAC de una ranura en el chasis.

Configuración de la red Fabric

La sección **Configuración de la red Fabric** muestra el tipo de red Fabric de entrada/salida que se instala para la red Fabric A. Una marca verde indica que la red Fabric está activada para FlexAddress. La función FlexAddress se utiliza para instalar direcciones WWN/MAC de ranuras persistentes y asignadas por el chasis en varias redes Fabric y ranuras en el chasis. Esta función se activa por red Fabric y por ranura.

NOTA: Para obtener más información acerca de la función FlexAddress, consulte Acerca de FlexAddress.

Visualización de la información de dirección WWN/MAC

Puede ver el inventario de las direcciones WWW/MAC para cada ranura de servidor o para todos los servidores en el chasis. El inventario incluye lo siguiente:

- Configuración de la red Fabric

NOTA:

- Fabric A muestra el tipo de red Fabric de entrada/salida instalada. Si la red Fabric A está activada, las ranuras desocupadas mostrarán direcciones MAC asignadas por el chasis para la red Fabric A.
- La controladora de administración de iDRAC no es una red Fabric, pero su FlexAddress es considerado como tal.
- SI la casilla de verificación asociada con un componente está seleccionada, significa que la red Fabric está activada para FlexAddress o FlexAddressPlus.

- Protocolo que se está utilizando en el puerto del adaptador NIC. Por ejemplo, LAN, ISCSI y FCoE.
- La configuración del nombre mundial (WWN) de Fiber Channel y las direcciones de control de acceso de medios (MAC) de una ranura en el chasis.
- Tipo de asignación de la dirección MAC y tipo de dirección activada actualmente: servidores asignados, FlexAddress MAC de identidad de E/S. Una marca de verificación de color negro indica el tipo de dirección activado, ya sea asignado por el servidor, asignado por el chasis o asignado de forma remota.
- Estado de las particiones de NIC para los dispositivos que admite la creación de particiones.

Puede ver el inventario de direcciones WWN/MAC a través de la interfaz web o la CLI de RACADM. Basado en la interfaz, puede filtrar la dirección MAC y saber qué dirección WWN/MAC está en uso para esa función o la partición. Si el adaptador tiene NPAR activado, puede ver qué particiones están activadas o desactivadas.

Mediante la interfaz web, puede ver la información de direcciones WWN/MAC para:

- Ranuras específicas: abra la página **FlexAddress**. Para ello, haga clic en **Descripción general del servidor → Ranura <x> → Configuración → FlexAddress**.
- Todas las ranuras y el servidor: abra la página **Resumen de WWN/MAC** . Para ello, haga clic en **Descripción general del servidor → Propiedades → WWN/MAC**.

Desde ambas páginas puede ver la información de Direcciones WWN/MAC en el modo básico o en el modo avanzado:

- **Modo básico**: en este modo, puede ver Ranura de servidor, Protocolo Fabri=c, direcciones WWN/MAC y Estado de la partición. Solamente se muestran las direcciones MAC activas en el cuadro Dirección de WWN/MAC. Puede filtrar utilizando cualquiera o todos los campos que se muestran:
- **Modo avanzado**: en este modo, puede ver todos los campos que se muestran en el modo básico y todos los tipos de MAC (asiganda por el servidor, asignada por Flex Address e identidad de E/S). Puede filtrar utilizando cualquiera o todos los campos que se muestran.

En el modo básico y en el modo avanzado, la información de las direcciones WWN/MAC se muestra en un formato contraído. Haga clic en el signo más + correspondiente a una ranura o haga clic en **Expandir/Contraer todos**) para ver la información de una ranura específica o de todas las ranuras.

También puede exportar la información de las direcciones WWN/MAC para todos los servidores del chasis en una carpeta local.

Para obtener información acerca de los campos, consulte la *ayuda en línea*.

Visualización de información básica sobre la dirección WWN_MAC mediante la interfaz web

Para ver la información de direcciones WWN/MAC de cada ranura del servidor o de todos los servidores en el chasis, en el modo básico:

1. Haga clic en **Descripción general del servidor → Propiedades → WWN/MAC**

   La página **Resumen de WWN/MAC** muestra la información sobre las direcciones WWN/MAC.

   De forma alternativa, haga clic en **Descripción general del servidor → Configuración → FlexAddress → Ranura <x>** Dirección WWN/MAC para ver la información de una ranura específica del servidor. Aparecerá la página **FlexAddress** .
2. En la tabla **Direcciones WWN/MAC**, haga clic en **Exportar** para guardar las direcciones WWN/MAC localmente.
3. Haga clic en el signo más  correspondiente a una ranura o haga clic en **Expandir/Contraer todo** para expandir o contraer la lista de atributos de una ranura específica o de todas las ranuras en la tabla Direcciones WWN/MAC.
4. En el menú desplegable **Ver**, seleccione **Básico**, para ver los atributos de las direcciones WWN/MAC en la vista de árbol.
5. Desde el menú desplegable **Ranura del servidor** , seleccione **Todos los servidores** o una ranura específica para ver los atributos de Direcciones WWN/MAC para todos los servidores o para servidores solamente en ranuras específicas, respectivamente.
6. Desde el menú desplegable de **Fabric**, seleccione uno de los tipos de red Fabric para ver los detalles de todos ellos o de tipos específicos de red Fabric de administración o de E/S asociados con los servidores.
7. Desde el menú desplegable **Protocolo**, seleccione **Todos los protocolos** o uno de los protocolos de red de la lista para ver todos los MACS o las direcciones MAC asociadas con el protocolo seleccionado.
8. En el campo **Direcciones WWN/MAC**, introduzca una dirección MAC parcial o toda la dirección MAC para ver únicamente las ranuras asociadas con la dirección MAC específica.
9. Desde el menú desplegable **Estado de partición**, seleccione el estado de las particiones para visualizar los servidores con el estado de partición seleccionado.

Para obtener información acerca de los campos, consulte la *ayuda en línea*.

Visualización de información avanzada sobre la dirección WWN/MAC mediante la interfaz web

Para ver información sobre la dirección WWN/MAC para cada ranura de servidor o todos los servidores del chasis, en el modo avanzado:

1. Haga clic en **Descripción general del servidor → Propiedades → WWN/MAC**

   La página **Resumen de WWN/MAC** muestra la información sobre la dirección WWN/MAC.
2. En el menú desplegable **Ver** , seleccione **Opciones avanzadas**, para ver los atributos de Direcciones WWN/MAC en la vista detallada.

   En la tabla **Direcciones WWN/MAC** se muestra: Ranura del servidor, Fabric, Protocolo, Direcciones WWN/MAC, Estado de partición, así como el tipo de asignación de la dirección MAC: Asignada por el servidor, FlexAddress o MAC de identidad de E/S. Una marca de verificación de color negro indica el

tipo de dirección activada, ya sea asignada por el servidor, asignada por el chasis o asignada de forma remota. MAC.

3. En la tabla **Direcciones WWN/MAC**, haga clic en **Exportar** para guardar las direcciones WWN/MAC localmente.
4. Haga clic en el + en una ranura o haga clic en **Expandir/contraer todo** para expandir o contraer la lista de atributos de una ranura específica o todas las ranuras en la tabla Direcciones WWN/MAC.
5. Desde el menú desplegable **Ranura del servidor** , seleccione **Todos los servidores** o una ranura específica para ver los atributos de Direcciones WWN/MAC para todos los servidores o para servidores solamente en ranuras específicas, respectivamente.
6. Desde menú desplegable **Fabric**, seleccione uno de los tipos de red Fabric para ver los detalles de todos ellos o de un tipo específico de red Fabric de administración o de E/S asociado con los servidores.
7. Desde el menú desplegable **Protocolo**, seleccione **Todos los protocolos** o uno de los protocolos de red de la lista para ver todos los MACS o las direcciones MAC asociadas con el protocolo seleccionado.
8. En el campo **Direcciones WWN/MAC**, introduzca la dirección MAC para ver únicamente las ranuras asociadas con la dirección MAC específica.
9. Desde el menú desplegable **Estado de partición**, seleccione el estado de las particiones para visualizar los servidores con el estado de la partición seleccionada.

   Si una partición en particular está desactivada, el estado que aparezca será **Desactivado** y la fila que muestra la partición aparece atenuada.

Para obtener información acerca de los campos, consulte la *ayuda en línea*.

Visualización de información sobre la dirección WWN/MAC mediante RACADM

Para ver la información sobre la dirección WWN/MAC para todos los servidores o servidores específicos mediante RACADM, utilice los subcomandos `getflexaddr` y `getmacaddress`.

Para mostrar Flexaddress para todo el chasis, use el siguiente comando de RACADM:

```
racadm getflexaddr
```

Para mostrar el estado de FlexAddress de una ranura particular, utilice el siguiente comando de RACADM:

```
racadm getflexaddr [-i <número de ranura>]
```

donde <*número de ranura*> es un valor de 1 a 4.

Para mostrar la dirección MAC de LOM o NDC, utilice el siguiente comando de RACADM:

```
racadm getmacaddress
```

Para mostrar la dirección MAC del chasis, use el siguiente comando RACADM:

```
racadm getmacaddress -m chassis
```

Para mostrar las direcciones MAC de iSCSI para todos los servidores, utilice el siguiente comando de RACADM:

```
racadm getmacaddress -t iscsi
```

Para mostrar las direcciones MAC de iSCSI para un servidor específico, utilice el siguiente comando de RACADM:

```
racadm getmacaddress [-m <módulo> [-x]] [-t iscsi]
```

Para mostrar el valor definido por el usuario de las direcciones MAC y WWN, utilice el siguiente comando de RACADM:

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

Para mostrar la consola de MAC/WWN asignada de todas las LOM o las tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c all
```

Para mostrar las direcciones WWN/MAC asignadas por el chasis, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c flexaddress
```

Para mostrar las direcciones MAC/WWN de todas las LOM o las tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -c factory
```

Para mostrar las direcciones MAC/WWN de iSCSI y Ethernet para todos los iDRAC, las LOM o las tarjetas intermedias, utilice el siguiente comando RACADM:

```
racadm getmacaddress -a
```

Para obtener más información acerca de los subcomandos **getflexaddr** y **getmacaddress**, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX).

Mensajes de comandos

En la siguiente tabla se muestran los comandos RACADM y los mensajes de situaciones comunes de FlexAddress.

Tabla 27. Comandos y mensajes de salida de FlexAddress

Situación	Comando	Mensaje de salida

La tarjeta SD en el módulo CMC activo está vinculada a otra etiqueta de servicio.	`$racadm featurecard -s`	`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`

Situación	Comando	Mensaje de salida
		válido de la dirección flexible>
La tarjeta SD en el módulo CMC activo está vinculada a la misma etiqueta de servicio.	`$racadm featurecard -s`	La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: vinculada
La tarjeta SD en el módulo CMC activo no está vinculada a ninguna etiqueta de servicio.	`$racadm featurecard -s`	La tarjeta de función insertada es válida y contiene las siguientes funciones FlexAddress: no vinculada

Función FlexAddress no activada en el chasis por algún motivo (no hay tarjeta SD insertada, tarjeta SD dañada, después de haber desactivado la función, tarjeta SD vinculada a otro chasis)	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		ERROR: Flexaddress feature is not active on the chassis (ERROR: La función Flexaddress no está activada en el chasis)

El usuario invitado intenta configurar FlexAddress en ranuras/redes Fabric.	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <slot#> <slotstate>]`
		ERROR: Insufficient user privileges to perform operation (ERROR: Privilegios de usuario insuficientes para realizar la operación)

Desactivar la función FlexAddress con el chasis encendido.	`$racadm feature -d -c flexaddress`	ERROR: Unable to deactivate the feature because the chassis is powered ON (ERROR: No se puede desactivar la función porque el chasis está encendido)
El usuario invitado intenta desactivar la función en el chasis.	`$racadm feature -d -c flexaddress`	ERROR: Insufficient user privileges to perform operation (ERROR: Privilegios de usuario insuficientes para realizar la operación)
Cambiar la configuración de FlexAddress de ranuras/redes Fabric mientras los módulos del servidor están encendidos.	`$racadm setflexaddr -i 1 1`	ERROR: Unable to perform the set operation because it affects a powered ON server (ERROR: No se puede realizar la operación de establecimiento porque afecta a un servidor encendido)

Situación	Comando	Mensaje de salida
Cambio de la configuración de Flexaddress en ranuras o redes Fabric cuando no hay instalada una licencia CMC Enterprise.	`$racadm setflexaddr -i<slotnum> <status>` `$racadm setflexaddr -f<FabricName> <status>`	`ERROR: SWC0242 : la licencia requerida no se encuentra o expiró. Obtenga la licencia correspondiente e inténtelo nuevamente, o bien comuníquese con su proveedor de servicio para más detalles.` NOTA: Para solucionar este problema, debe contar con una licencia de **Activación de FlexAddress**.

CONTRATO DE LICENCIA DE SOFTWARE DE DELL FlexAddress

El presente documento es un contrato legal entre usted, el usuario, y Dell Products, L.P. o Dell Global B.V. ("Dell"). Este contrato cubre todo el software que se distribuye con el producto Dell, para el que no existe un contrato de licencia diferente entre usted y el fabricante o el propietario del software (de manera colectiva, el "Software"). Este contrato no es para la venta de Software o de cualquier otra propiedad intelectual. Todos los derechos de título y propiedad intelectual del Software y para este pertenecen al fabricante o propietario del Software. Todos los derechos no otorgados expresamente bajo este contrato son derechos reservados por el fabricante o propietario del Software. Al abrir o romper el sello de los paquetes de Software, instalar o descargar el Software, o utilizar el Software que se ha cargado previamente o que se incluye en el producto, usted acepta estar sujeto a los términos de este contrato. Si no acepta estos términos, devuelva de inmediato todos los artículos de Software (discos, material escrito y embalaje) y elimine el Software cargado previamente en el producto o incorporado en él.

Únicamente podrá utilizar una copia de Software por equipo a la vez. Si dispone de varias licencias de Software, podrá utilizar en cualquier momento tantas copias como licencias tenga. Con el término "utilizar" se entiende cargar el Software en la memoria temporal o en el almacenamiento permanente del equipo. La instalación del Software en un servidor de red con el único fin de distribuirlo a otros equipos no significará "utilizarlo" siempre y cuando disponga de una licencia independiente para cada equipo en el que distribuya el Software. Debe asegurarse de que la cantidad de personas que utilicen el Software instalado en un servidor de red no sea superior a la cantidad de licencias que disponga. Si la cantidad de usuarios del Software instalado en un servidor de red supera el número de licencias, deberá adquirir licencias adicionales hasta que la cantidad de licencias iguale la cantidad de usuarios, antes de permitir que estos utilicen el Software. Si usted es un cliente comercial de Dell o un socio de Dell, por el presente concede a Dell o a un representante seleccionado por Dell, el derecho a realizar una auditoría sobre el uso que usted hace del Software durante el horario laboral normal, acepta cooperar con Dell en dicha auditoría y proporcionarle todos los informes relacionados razonablemente con el uso que hace del Software. La auditoría se limitará a la verificación del cumplimiento de los términos de este contrato por su parte.

El Software está protegido por las leyes de derechos de autor de Estados Unidos y por tratados internacionales. Únicamente podrá hacer una copia del Software para disponer de una copia de

seguridad o para archivarlo o transferirlo a un solo disco duro, siempre que guarde el original solo para fines de respaldo o de archivado. No puede alquilar o arrendar el software 240 mediante FlexAddress y las tarjetas FlexAddress Plus ni copiar los materiales impresos que se adjuntan con él, pero sí puede transferir el software y todos los materiales adjuntos de manera permanente como parte de la venta o transferencia del producto Dell siempre y cuando no se quede con ninguna copia y los destinatarios acepten los términos de este documento. Cualquier transferencia deberá incluir la actualización más reciente y todas las versiones anteriores. No se permite aplicar técnicas de ingeniería inversa, descompilar o desensamblar el Software. Si el paquete que acompaña a su equipo contiene CD, disquetes de 3.5" o de 5.25", podrá utilizar únicamente los adecuados para su equipo. No podrá utilizar los discos en otro equipo o red, ni prestarlos, alquilarlos, arrendarlos o transferirlos a otro usuario, salvo según lo permita el presente contrato.

GARANTÍA LIMITADA

Dell garantiza que los discos de Software no presentarán defectos en los materiales ni en su fabricación, siempre que se realice un uso normal, durante noventa (90) días a partir de la fecha de recepción. Esta garantía se limita a usted y no es transferible. Las garantías implícitas se limitan a noventa (90) días a partir de la fecha de recepción del Software. En algunas jurisdicciones no existen limitaciones en la vigencia de la garantía implícita, de modo que esta limitación puede no ser aplicable en su caso. La responsabilidad total de Dell y de sus proveedores, así como su remedio exclusivo, se limitará (a) a la devolución del importe pagado por el Software o (b) a la sustitución de los discos que no cumpla esta garantía y que usted envíe a Dell con un número de autorización de devolución, por su cuenta y riesgo. Esta garantía limitada se anulará si se daña el disquete como resultado de accidentes, abuso, usos incorrectos, tareas de mantenimiento o modificaciones por parte de alguna persona que no pertenezca a Dell. La garantía cubre los discos de reemplazo durante el período restante de la garantía original o durante treinta (30) días, lo que resulte mayor.

Dell NO garantiza que las funciones del Software satisfarán sus necesidades o que el funcionamiento del Software no se interrumpirá o no tendrá errores. Usted asume la responsabilidad de seleccionar el Software para lograr los resultados que espera, así como del uso y de los resultados obtenidos con el Software.

DELL, EN SU NOMBRE Y EN EL DE SUS PROVEEDORES, NO SE HARÁ RESPONSABLE DE NINGUNA OTRA GARANTÍA, EXPLÍCITA O IMPLÍCITA, INCLUYENDO PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN ESPECÍFICO, POR LO QUE SE REFIERE AL SOFTWARE Y A TODOS LOS MATERIALES ESCRITOS QUE LO ACOMPAÑAN. Esta garantía limitada le otorga derechos legales específicos; es posible que usted tenga otros derechos, que varían en función de la jurisdicción.

EN NINGÚN CASO DELL O SUS PROVEEDORES SERÁN RESPONSABLES DE LOS DAÑOS QUE PUEDAN OCURRIR (LO QUE INCLUYE, SIN LÍMITE, LOS DAÑOS POR PÉRDIDA DE BENEFICIOS, INTERRUPCIÓN O PÉRDIDA DE INFORMACIÓN DEL NEGOCIO O CUALQUIER OTRA PÉRDIDA PECUNIARIA) A CAUSA DEL USO O LA INCAPACIDAD DE UTILIZAR EL SOFTWARE, AUNQUE SE LE NOTIFIQUE DE LA POSIBILIDAD DE TALES DAÑOS. Puesto que algunas jurisdicciones no permiten la exclusión o limitación de responsabilidad por daños resultantes o accidentales, la limitación anteriormente mencionada puede no ser aplicable en su caso.

SOFTWARE DE CÓDIGO DE FUENTE ABIERTO

Una parte de este CD puede contener software de código de fuente abierto, que puede utilizar bajo los términos y condiciones de la licencia específica bajo la cual el software se distribuye.

ESTE SOFTWARE DE CÓDIGO DE FUENTE ABIERTO SE DISTRIBUYE CON LA INTENCIÓN DE QUE PUEDA SER ÚTIL, PERO SE PROPORCIONA "TAL CUAL" SIN NINGUNA GARANTÍA EXPLÍCITA O EXPRESA; INCLUYENDO PERO SIN LIMITARSE A LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O IDONEIDAD PARA UN FIN ESPECÍFICO. BAJO NINGUNA CIRCUNSTANCIA, DELL, LOS TITULARES DE LOS DERECHOS DE AUTOR O LOS CONTRIBUYENTES SE HARÁN RESPONSABLES DE DAÑOS DIRECTOS, INDIRECTOS, ACCIDENTALES, ESPECIALES, EJEMPLARES O CONSECUENTES (LO QUE INCLUYE, SIN LIMITARSE A, LA ADQUISICIÓN DE SERVICIOS O PRODUCTOS SUSTITUTOS; PÉRDIDA DE USO, DATOS O BENEFICIOS; O LA INTERRUPCIÓN DEL NEGOCIO) SIN IMPORTAR LA MANERA EN QUE SE HAYAN PRODUCIDO NI LA TEORÍA DE RESPONSABILIDAD, YA SEA BAJO CONTRATO, RESPONSABILIDAD ESTRICTA O DELICTIVA (LO QUE INCLUYE LA NEGLIGENCIA O SIMILARES) QUE SE HAYAN OCASIONADO POR EL USO DE ESTE SOFTWARE, INCLUSO SI SE NOTIFICÓ SOBRE LA POSIBILIDAD DE DICHO DAÑO.

DERECHOS LIMITADOS DEL GOBIERNO DE EE. UU.

El software y la documentación son "artículos comerciales" tal como se define dicho término en 48 C.F.R. 2.101, que constituyen "software informático comercial" y "documentación de software informático comercial" según se utilizan dichos términos en 48 C.F.R. 12.212. En conformidad con 48 C.F.R. 12.212 y 48 C.F.R. 227.7202-1 a 227.7202-4, todos los usuarios finales del gobierno de EE. UU. adquieren el software y la documentación únicamente con los derechos estipulados en este documento.

El contratante/fabricante es Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

GENERAL

Esta licencia permanecerá vigente hasta que finalice. Dicha finalización se llevará a cabo según las condiciones estipuladas anteriormente o si usted no cumple alguno de estos términos. Una vez que haya finalizado, usted acepta que procederá a la destrucción del Software y de los materiales que lo acompañan, así como de todas las copias de estos. Este contrato está regulado por las leyes del estado de Texas. Las cláusulas de este contrato son independientes. Si se considera que alguna cláusula no es aplicable, dicha consideración no afectará la aplicabilidad del resto de las cláusulas, los términos o las condiciones de este contrato. Este contrato es vinculante para los sucesores y cesionarios. Tanto Dell como usted aceptan renunciar, según lo máximo permitido por la ley, a cualquier derecho a juicio con jurado con respecto al Software o a este contrato. Como esta renuncia de derechos puede no ser efectiva en ciertas jurisdicciones, es posible que no se aplique en su caso. Usted reconoce que ha leído el presente contrato, que lo entiende y acepta estar sujeto a sus términos, y que esta es la declaración completa y exclusiva del contrato entre usted y Dell con respecto al Software.

13

Administración de redes Fabric

El chasis admite el tipo de red Fabric A. Esta red es utilizada por el único módulo de E/S y está siempre conectada a los adaptadores Ethernet integrados de los servidores.

El chasis cuenta con un solo módulo de E/S, que funciona como módulo de pasada o conmutación. El módulo de E/S se clasifica en el grupo A.

El módulo de E/S del chasis utiliza una ruta de acceso a datos discreta denominada **Fabric** que recibe el nombre A. La red Fabric A admite solo Ethernet. Cada servidor del adaptador de E/S (tarjeta mezzanine o LOM) puede tener dos o cuatro puertos, según su capacidad. Las ranuras de la tarjeta mezzanine están ocupadas por las tarjetas de extensión PCIe que están conectadas a las tarjetas PCIe (y no a los módulos de E/S). Al implementar las redes Ethernet, iSCSI o FibreChannel, expanda los vínculos redundantes por los tramos uno y dos para obtener la máxima disponibilidad. El módulo de E/S discreto está identificado con un identificador de red Fabric.

NOTA: En la CLI del CMC, al módulo de E/S se lo conoce por la convención "conmutador".

Situación de encendido por primera vez

Cuando el chasis está conectado y encendido, el módulo de E/S tiene prioridad con respecto a los servidores. Se permite que el M. E/S se encienda antes que los demás. En este momento, no se realiza la verificación de sus tipos de red Fabric.

Una vez que se encienden los M. E/S, se encienden los servidores y, a continuación, el CMC verifica la congruencia de red Fabric en los servidores.

Se permite un módulo de paso y uno de conmutación en el mismo grupo, siempre y cuando sus redes Fabric sean idénticas. Los módulos de conmutación y de paso pueden existir en el mismo grupo, incluso si fueron fabricados por proveedores distintos.

Supervisión de la condición del módulo de E/S

Para obtener información sobre cómo supervisar la condición del módulo de E/S, consulte Visualización de la información y el estado de condición del M. E/S.

Configuración de los valores de red para módulos de E/S

Es posible especificar los valores de red para la interfaz usada para administrar el módulo de E/S. Para los conmutadores de Ethernet, se configura el puerto de administración fuera de banda (dirección IP). El puerto de administración en banda (es decir, VLAN1) no se configura mediante esta interfaz.

Antes de configurar los valores de red para los módulos de E/S, asegúrese de que el módulo de E/S esté encendido.

Para configurar los valores de red del módulo de E/S en el grupo A, debe contar con privilegios de administrador de la red Fabric A.

NOTA: En los conmutadores de Ethernet, las direcciones IP de administración en banda (VLAN1) y fuera de banda no pueden ser las mismas ni estar en la misma red; esto provoca que no se configure la dirección IP fuera de banda. Consulte la documentación sobre el módulo de E/S para la dirección IP de administración en banda predeterminada.

NOTA: No intente configurar los valores de la red del módulo de E/S para módulos de paso de Ethernet y conmutadores de Infiniband.

Configuración de los valores de red para los módulos de E/S mediante la interfaz web del CMC

Para configurar los valores de red para los módulos de E/S:

1. En el panel izquierdo, haga clic en **Descripción general del chasis**, haga clic en **Descripción general del módulo de E/S** y, a continuación, haga clic en **Configuración**. Como alternativa, para configurar los valores de red del único módulo de E/S disponible que es **A**, haga clic en **Una Ethernet de gigabits** y, a continuación, haga clic en **Configuración**.

   En la página **Configurar valores de red para los módulos de E/S**, escriba los datos adecuados y haga clic en Aplicar.
2. Si está permitido, escriba la contraseña root, la cadena de comunicad de SNMP RO y la dirección IP del servidor Syslog para el módulo de E/S. Para obtener más información acerca de las descripciones de los campos, consulte *Online Help* (Ayuda en línea).

   NOTA: La dirección IP establecida en los módulos de E/S a partir del CMC no se guarda en la configuración de inicio permanente del conmutador. Para guardar la configuración de la dirección IP de forma permanente, debe introducir el comando `connect switch` o el comando de RACADM `racadm connect switch` o bien, usar una interfaz directa a la interfaz gráfica de usuario del módulo de E/S para guardar esta dirección en el archivo de configuración de inicio.
3. Haga clic en **Apply (Aplicar)**.

   Los valores de red se configuran para los módulos de E/S.

   NOTA: Si está permitido, es posible restablecer las VLAN, las propiedades de la red y los puertos de E/S a sus valores de configuración predeterminados.

Configuración de los valores de red para los módulos de E/S mediante RACADM

Para configurar los valores de la red para un módulo de E/S mediante RACADM, establezca la fecha y la hora. Consulte la sección del comando deploy en *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de de Chassis Management Controller para PowerEdge VRTX).

Es posible establecer el nombre de usuario, la contraseña y la cadena SNMP para un módulo de E/S mediante el comando deploy de RACADM:

```
racadm deploy -m switch -u <username> -p <password>

racadm deploy -m switch -u -p <password> -v SNMPv2 <snmpCommunityString> ro

racadm deploy -a [server|switch] -u <username> -p <password>
```

Administración de la operación de control de alimentación para los módulos de E/S

Para obtener información para establecer la operación de control de alimentación para los módulos de E/S, consulte Executing Power Control Operations on the IOM (Ejecución de las operaciones de control de alimentación en el M. E/S).

Activación o desactivación del parpadeo del LED para los módulos de E/S

Para obtener información sobre cómo activar el parpadeo del LED para los módulos de E/S, consulte Configuring LEDs to Identify Components on the Chassis (Configuración de los LED para identificar componentes en el chasis).

14

Administración y supervisión de la alimentación

El chasis PowerEdge VRTX es el gabinete de servidor modular más eficiente en términos de energía. Su diseño permite incluir ventiladores y suministros de energía de alta eficacia y está optimizado para que el aire circule con mayor facilidad por el sistema; además, contiene componentes con consumo mejorado de la energía en todo el gabinete. El diseño de hardware optimizado complementa las sofisticadas capacidades de administración de la energía integradas en el Chassis Management Controller (CMC), los suministros de energía y el iDRAC para mejorar aún más la eficiencia de la alimentación y permitir el control total del entorno de alimentación.

Las funciones de administración de la alimentación de PowerEdge VRTX permiten a los administradores configurar el gabinete de modo tal que se reduzca el consumo de alimentación y se ajuste la alimentación según lo requiera el entorno específico.

El gabinete modular PowerEdge VRTX consume energía de corriente alterna (CA) y distribuye la carga por todas las unidades de suministro de energía (PSU) internas. El sistema puede producir hasta 4800 vatios de CA que se asignan a los módulos del servidor y la infraestructura de gabinete asociada. No obstante, esta capacidad puede variar en función de la política de redundancia que seleccione.

El gabinete PowerEdge VRTX se puede configurar para cualquiera de las dos políticas de redundancia que afectan el comportamiento de la unidad de suministro de energía y determinan la manera en la que se notifica a los administradores el estado de redundancia del chasis.

Además, puede controlar la administración de la alimentación mediante el centro **OpenManage Power Center (OMPC)**. Cuando OMPC controla la alimentación de manera externa, CMC todavía mantiene las siguientes funciones:

- Política de redundancia
- Registro remoto de la alimentación
- Conexión dinámica de suministros de energía

El centro OMPC administra, entonces, lo siguiente:

- Alimentación del servidor
- Prioridad de los servidores
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

NOTA: La entrega real de alimentación se basa en la configuración y en la carga de trabajo.

Puede utilizar la interfaz web del CMC y RACADM para administrar y configurar los controles de alimentación en el CMC:

- Ver las asignaciones, el consumo y el estado de alimentación del chasis, de los servidores y de las unidades de suministro de energía.

- Configurar el presupuesto de alimentación y la política de redundancia del chasis.
- Ejecutar operaciones de control de alimentación (encendido, apagado, restablecimiento del sistema, ciclo de encendido) en el chasis.

Políticas de redundancia

La política de redundancia es un conjunto configurable de propiedades que determina la forma en que el CMC administra la alimentación al chasis. Las siguientes políticas de redundancia son configurables con conexión dinámica de unidad de suministro de energía o sin ella:

- Redundancia de cuadrícula
- Redundancia del suministro de energía

Política de redundancia de la red eléctrica

El objetivo de la política de redundancia de cuadrícula 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 o el suministro o bien, en la propia unidad de suministro de energía.

Cuando se configura un sistema para tener redundancia de cuadrícula, las unidades de suministro de energía se dividen en redes eléctricas: las unidades de las ranuras 1 y 2 se encuentran en la primera red eléctrica, en tanto que las unidades de las ranuras 3 y 4 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 funcionará sin que haya degradación. La redundancia de cuadrícula también tolera las fallas de las unidades de suministro de energía individuales.

NOTA: Dado que una de las funciones de la redundancia de cuadrícula es proporcionar una operación perfecta del servidor a pesar de cualquier falla que se produzca en toda una red eléctrica, la mayor parte de la alimentación se pone a disposición del mantenimiento de la redundancia de cuadrícula cuando las capacidades de las dos redes eléctricas son aproximadamente iguales.

NOTA: La redundancia de cuadrícula solo se cumple cuando los requisitos de carga no superan la capacidad de la red eléctrica más débil.

Niveles de redundancia de la red eléctrica

La configuración mínima necesaria para tener redundancia de cuadrícula es tener una unidad de suministro de energía en cada red eléctrica. Es posible definir configuraciones adicionales con cada combinación que tenga al menos una unidad de suministro de energía en cada red eléctrica. Sin embargo, para que el máximo nivel de energía esté disponible para su uso, la energía total de las unidades de suministro de energía de cada red eléctrica debe ser lo más similar posible. El límite máximo de energía mientras se mantiene la redundancia de cuadrícula es la energía disponible en la red eléctrica más débil.

Si el CMC no puede mantener la redundancia de cuadrícula, se envían alertas de correo electrónico y/o SNMP a los administradores, siempre que el suceso Redundancia perdida esté configurado para el envío de alertas.

En el caso de una sola unidad de suministro de energía que no funcione con esta configuración, las unidades de suministro de energía restantes en la cuadrícula que causa el problema se marcan como en

línea. En ese estado, las unidades de suministro de energía de la cuadrícula redundante si no están en estado de falla, ayudan con el funcionamiento del sistema sin interrupción. Si una unidad de suministro de energía deja de funcionar, la condición del chasis aparece como no crítica. Si la cuadrícula más pequeña no puede admitir todas las asignaciones de energía del chasis, entonces se informa el estado de redundancia de la cuadrícula como **No** y la condición del chasis aparece como **Crítica**.

Política de redundancia de suministro de energía

La política de redundancia de suministro de energía es útil cuando las redes de energía redundante no están disponibles, pero es posible que desee estar protegido contra una falla de una única unidad de suministro de energía que deje fuera de servicio a los servidores en un gabinete modular. La unidad de suministro de energía de mayor capacidad se mantiene en reserva en línea para este propósito. Esto forma un grupo de redundancia de suministro de energía.

Las demás unidades de suministro de energía además de las necesarias para alimentación y redundancia siguen disponibles y se agregan al grupo en caso de falla.

A diferencia de la redundancia de cuadrícula, cuando se selecciona la redundancia de suministro de energía, el CMC no requiere que las unidades de suministro de energía estén presentes en ninguna posición específica de las ranuras de las unidades de suministro de energía.

NOTA: La conexión dinámica del suministro de energía (DPSE) permite poner en espera las unidades de suministro de energía. El estado En espera indica una 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.

Conexión dinámica de suministros de energía

De forma predeterminada, el modo de conexión dinámica de suministros de energía (DPSE) está desactivado. DPSE ahorra energía al optimizar la eficiencia energética de las unidades de suministro de energía que suministran energía al chasis. Esto también produce un aumento de la vida de las unidades de suministro de energía y reduce la generación de calor. Para usar esta función, el usuario debe tener una licencia Enterprise.

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 a mayor capacidad, esto mejora su eficiencia al mismo tiempo que mejora la longevidad de las unidades de suministro de energía en espera.

Para operar las unidades de suministro de energía restantes en su máxima eficiencia, use los siguientes modos de redundancia de alimentación:

- El modo **Redundancia de las unidades de suministro de energía** con DPSE 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 las unidades 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 eléctrica de CA.
- El modo de **Redundancia de cuadrícula** con DPSE, en donde por lo menos dos unidades de suministro de energía están activas, una en cada red de energía. La redundancia de cuadrícula equilibra también la eficiencia y la disponibilidad máxima para una configuración de gabinete modular parcialmente cargado.

- La desactivación de DPSE proporciona la más baja eficiencia ya que las cuatro fuentes están activas y comparten la carga, lo cual produce una utilización más baja de cada suministro de energía.

La DPSE puede activarse para las dos configuraciones de redundancia de suministro de energía explicadas anteriormente: **Redundancia de suministro de energía** y **Redundancia de cuadrícula**.

NOTA: En los modos de una configuración de dos unidades de suministro de energía, la carga del servidor puede evitar que cualquier unidad de suministro de energía cambie al modo En espera.

- En una configuración de **Redundancia de suministro de energía**, además de las unidades de suministro de energía requeridas para alimentar el gabinete, el gabinete mantiene siempre una unidad de suministro de energía adicional encendida e identificada como **En línea**. La utilización de energía se supervisa y una unidad de suministro de energía se puede colocar en el estado En espera en función de la carga del sistema total. En una configuración de cuatro unidades de suministro de energía, un mínimo de dos unidades de suministro de energía están 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 adecuar la pérdida de una unidad de suministro de energía en línea y aún tener suficiente energía para los módulos de servidor instalados. La pérdida de la unidad de suministro de energía en línea hará que una unidad en espera 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 cuadrícula**, todas las unidades de suministro de energía están activas 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 estado **En línea** de las unidades de suministro de energía en una red eléctrica refleja el modo de la otra red eléctrica, el gabinete puede sobrellevar la pérdida de alimentación de una red eléctrica completa sin interrumpir la alimentación del gabinete.

  Un aumento de la demanda de energía en la configuración de **Redundancia de cuadrícula** 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 cuadrícula.

  NOTA: Con DPSE en estado activado, si la demanda de energía aumenta en los dos modos de políticas de redundancia de alimentación, las unidades de suministro de energía en espera se colocan **En línea** para recuperar energía.

Configuración predeterminada de redundancia

Como se muestra en la tabla a continuación, la configuración predeterminada de redundancia de un chasis depende del número de unidades de suministro de energía que contiene.

Tabla 28. Configuración predeterminada de redundancia

Configuración de unidades de suministro de energía	Política de redundancia predeterminada	Valor predeterminado de la conexión dinámica de unidades de suministro de energía
Dos unidades de suministro de energía	Redundancia de CC	Desactivado
Cuatro unidades de suministro de energía	Redundancia de CC	Desactivado

Redundancia de cuadrícula

En el modo de redundancia de cuadrícula con cuatro unidades de suministro de energía, las cuatro unidades están activas. Las dos unidades deben conectarse a una red eléctrica de alimentación de CA, en tanto que las otras dos unidades se conectan a las otras redes eléctricas de alimentación de CA.

PRECAUCIÓN: Para evitar una falla del sistema y para que la redundancia de cuadrícula funcione de manera eficaz, debe haber un conjunto equilibrado de unidades de suministro de energía correctamente cableadas a redes de CA independientes.

Si una red de CA falla, las unidades de suministro de energía de la red de CA en funcionamiento tomarán el control sin que se interrumpan los servidores o la infraestructura.

PRECAUCIÓN: En el modo de redundancia de cuadrícula, debe tener 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 cuadrícula no será posible.

Redundancia del suministro de energía

Cuando se activa la redundancia de suministro de energía, una de las unidades de suministro de energía del chasis se mantiene como repuesto, lo cual garantiza que la falla de una de las unidades no ocasione que se apaguen los servidores o el chasis. El modo de redundancia de suministro de energía requiere un mínimo de dos unidades de suministro de energía. Si existen unidades de suministro de energía adicionales, serán utilizadas para mejorar la eficiencia energética del sistema cuando la DPSE esté activada. Las fallas posteriores a una pérdida de redundancia pueden provocar que los servidores del chasis se apaguen.

Presupuesto de alimentación para módulos de hardware

El CMC ofrece un servicio de presupuesto de alimentación que le permite configurar el presupuesto de alimentación, la redundancia y la alimentación dinámica para el chasis.

El servicio de administración de la alimentación permite optimizar el consumo de alimentación y reasignar la alimentación a diferentes módulos en función de la demanda.

El CMC mantiene un presupuesto de alimentación para el gabinete que reserva la potencia necesaria para todos los servidores y componentes instalados.

El CMC asigna alimentación a la infraestructura del CMC y los servidores en el chasis. La infraestructura del CMC consta de componentes en el chasis, como ventiladores, módulos de E/S y adaptadores de almacenamiento, tarjetas PCIe, discos físico y placa principal. El chasis puede tener hasta cuatro servidores que se comunican con éste a través del iDRAC. Para obtener más información, consulte *iDRAC User's Guide* (Guía del usuario de iDRAC) en **dell.com/support/manuals**.

El iDRAC proporciona al CMC el requisito de envolvente de potencia antes de encender el servidor. La envolvente de potencia consiste en los requisitos de alimentación máxima y mínima para mantener el servidor en funcionamiento. El cálculo inicial del iDRAC se basa en la comprensión inicial de los componentes en el servidor. Después de iniciar el funcionamiento y de detectar otros componentes, el iDRAC puede aumentar o reducir sus requisitos de alimentación iniciales.

Cuando se enciende un servidor en un gabinete, el software del iDRAC vuelve a calcular los requisitos de alimentación y solicita el cambio correspondiente en la envolvente de potencia.

El CMC suministra la alimentación solicitada al servidor y la potencia eléctrica asignada se resta del presupuesto disponible. Una vez que se otorga una solicitud de alimentación, el software del iDRAC del servidor supervisa continuamente el consumo de alimentación real. En función de los requisitos de la alimentación real, la envolvente de potencia del iDRAC puede cambiar al cabo de un período de tiempo. iDRAC solicita una configuración de alimentación si los servidores utilizan de forma total la alimentación asignada.

En condiciones de carga pesada, el funcionamiento de los procesadores del servidor puede degradarse para garantizar que el consumo de alimentación se mantenga por debajo del valor de Límite de alimentación de entrada del sistema configurado por el usuario.

El gabinete PowerEdge VRTX puede suministrar alimentación suficiente para un rendimiento máximo de la mayoría de las configuraciones de servidores, pero varias configuraciones de servidores disponibles no consumen la alimentación máxima que el gabinete puede suministrar. Para ayudar a los centros de datos a asignar alimentación a sus gabinetes, PowerEdge VRTX permite al usuario especificar un límite de energía de entrada del sistema para garantizar que la alimentación de CA general del chasis permanezca dentro del punto umbral otorgado. El CMC garantiza primero que haya suficiente alimentación disponible para hacer funcionar los ventiladores, los módulos de E/S, los adaptadores de almacenamiento, las unidades de discos físicos, la placa principal y el CMC propiamente dicho. Esta asignación de alimentación se denomina energía de entrada asignada a la infraestructura del chasis. Después de la infraestructura del chasis, los servidores en un gabinete se encienden. Cualquier intento de establecer un límite de energía de entrada del sistema menor a la carga de alimentación no se realizará con éxito. La carga de alimentación es la suma de alimentación asignada a la infraestructura y la alimentación mínima asignada para los servidores conectados.

NOTA: Para usar la función de límite de energía, el usuario debe tener una licencia Enterprise.

Si para el presupuesto total de alimentación es necesario permanecer por debajo del valor de *Límite de alimentación de entrada del sistema*, el CMC asignará a los servidores un valor menor que la alimentación máxima solicitada. Se asigna alimentación a los servidores en función de la configuración de *Prioridad del servidor*, en la que los servidores con prioridad más alta reciben el máximo de alimentación, los servidores con prioridad 2 reciben alimentación después de los servidores con prioridad 1, y así sucesivamente. Los servidores de menor prioridad pueden recibir menos alimentación de acuerdo con la *Capacidad de alimentación máxima de entrada del sistema* y el valor de *Límite de alimentación de entrada del sistema* que el usuario haya configurado.

Los cambios de configuración, como un servidor adicional, HDD compartidos o tarjetas PCIe en el chasis, pueden requerir que se deba aumentar el *Límite de alimentación de entrada del sistema*. Las necesidades energéticas en un gabinete modular aumentan también cuando cambian las condiciones térmicas y es necesario que los ventiladores funcionen a mayor velocidad, lo que provoca que consuman energía adicional. La colocación de módulos de E/S y adaptadores de almacenamiento, tarjetas PCIe, discos físicos, placa principal, número, tipo y configuración de unidades de suministro de energía aumentan también las necesidades energéticas del gabinete modular. Los servidores consumen una cantidad bastante pequeña de energía cuando se apagan para mantener 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 5000 vatios para permitir el encendido de servidores adicionales.

Los cambios en el gabinete modular que reducen la asignación de alimentación son:

- El servidor se apagó
- El módulo de E/S se apagó
- Los adaptadores de almacenamiento, las tarjetas PCIe, la unidad de disco físico y la placa principal se apagaron
- Transición del chasis al estado apagado

Los usuarios pueden reconfigurar el *Límite de alimentación de entrada del sistema* cuando el chasis está encendido o apagado.

Configuración de la prioridad de alimentación de ranura del servidor

El CMC permite que los usuarios establezcan una prioridad de alimentación para cada una de las 4 ranuras de servidores de un gabinete. Los valores de prioridad son de 1 (la más alta) a 9 (la más baja). Estos valores se asignan a las ranuras del chasis y todo servidor insertado en esa ranura heredará la prioridad de la ranura. El CMC utiliza la prioridad de ranura para administrar alimentación con preferencia para los servidores de más alta prioridad en el gabinete.

Según el valor predeterminado de prioridad de ranura de servidor, la alimentación se distribuye por igual a todas las ranuras. El cambio de prioridades de ranura permite a los administradores priorizar a qué servidores se les dará preferencia al asignar alimentación. Si los módulos de servidor más importantes se dejan con la prioridad de ranura predeterminada de 1 y los módulos de servidor menos críticos se cambian a un valor más bajo de prioridad de 2 o un número mayor, primero se dará alimentación a los módulos de servidor de prioridad 1. Estos servidores de prioridad más alta obtendrían su asignación máxima de alimentación, mientras que a los servidores de prioridad más baja no se les asignaría suficiente alimentación para funcionar a su máximo rendimiento o no se encenderían en absoluto. Esto depende del valor mínimo en el que se establezca el límite de alimentación de entrada del sistema y los requisitos de alimentación del servidor.

Si un administrador enciende manualmente los módulos de servidor de baja prioridad antes que los de prioridad más alta, los módulos de servidor de prioridad baja serán los primeros módulos a los que se les disminuya su asignación de alimentación a su valor mínimo, a fin de abastecer a los servidores de mayor prioridad. Por lo tanto, cuando se agota la alimentación disponible para la asignación, el CMC retira alimentación de los servidores de prioridad inferior o igual hasta que alcanzan el nivel mínimo de alimentación.

NOTA: Los módulos de E/S, los ventiladores, la placa principal, las unidades de disco físico y los adaptadores de almacenamiento reciben la mayor prioridad. El CMC requiere solo la alimentación de los dispositivos de prioridad baja para satisfacer las necesidades de alimentación de un servidor o dispositivo de prioridad alta.

Asignación de niveles de prioridad a los servidores

Cuando se requiere alimentación adicional, los niveles de prioridad de los servidores determinan los servidores desde donde el CMC extrae energía.

NOTA: La prioridad que se asigna a un servidor está vinculada a la ranura y no al servidor en sí. Si traslada el servidor a una nueva ranura, debe reconfigurar la prioridad para la ubicación de la nueva ranura.

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Asignación de niveles de prioridad a los servidores mediante la interfaz web del CMC

Para asignar niveles de prioridad:

1. En el panel izquierdo, haga clic en **Descripción general del servidor → Alimentación → Prioridad**.
   La página **Prioridad de los servidores** muestra todos los servidores del chasis.
2. En el menú desplegable **Prioridad**, seleccione un nivel de prioridad (del 1 al 9, en donde 1 es la prioridad más alta) para uno, varios o todos los servidores. El nivel predeterminado es 1. Puede asignar la misma prioridad para varios servidores.
3. Haga clic en **Apply (Aplicar)** para guardar los cambios.

Asignación de niveles de prioridad a los servidores mediante RACADM

Abra una consola de texto de serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <slot number> <priority level>
```

donde <*slot number*> (de 1 a 4) se refiere a la ubicación del servidor y <*priority level*> es un valor entre 1 y 9.

Por ejemplo, para establecer el nivel de prioridad en 1 para el servidor en la ranura 4, escriba el siguiente comando:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 4 1
```

Visualización del estado del consumo de alimentación

El CMC proporciona el consumo real de alimentación de entrada para todo el sistema.

Visualización del estado del consumo de alimentación mediante la interfaz web del CMC

En el panel izquierdo, haga clic en **Descripción general del chasis → Alimentación → Supervisión de alimentación**. La página Supervisión de alimentación muestra la condición de alimentación, el estado de alimentación del sistema, las estadísticas de alimentación en tiempo real y las estadísticas de energía en tiempo real. Para obtener más información, consulte la *Ayuda en línea*.

NOTA: También puede ver el estado de redundancia de alimentación en la opción Suministros de energía.

Visualización del estado del consumo de alimentación con el comando RACADM

Para ver el estado del consumo de alimentación con el comando RACADM:

Abra una consola de texto de serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getpminfo
```

Visualización del estado de presupuesto de alimentación mediante la interfaz web del CMC

Para ver el estado de presupuesto de alimentación mediante la interfaz web del CMC, en el panel izquierdo vaya a **Descripción general del chasis** y haga clic en **Alimentación** → **Estado de presupuesto**. La página **Estado de presupuesto de alimentación** muestra la configuración de la política de alimentación del sistema, los detalles del presupuesto de alimentación, el presupuesto asignado para los módulos del servidor y los detalles del suministro de energía del chasis. Para obtener más información, consulte la *Ayuda en línea*.

Visualización del estado del presupuesto de alimentación mediante RACADM

Abra una consola de texto de serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getpbinfo
```

Para obtener más información sobre **getpbinfo**, incluidos los detalles de salida, consulte la sección del comando **getpbinfo** en la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia sobre la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Estado de redundancia y condición general de la alimentación

El estado de redundancia es un factor determinante de la condición general de la alimentación. Cuando se establece la política de redundancia de alimentación, por ejemplo, en Redundancia de cuadrícula, y el estado de redundancia indica que el sistema funciona con redundancia, la condición general de la alimentación normalmente será **En buen estado**. Sin embargo, si no se satisfacen las condiciones para operar con redundancia de cuadrícula, el estado de la 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 cuadrícula o de esta última a otra. Por lo tanto, configurar la política de redundancia podría ocasionar inmediatamente una pérdida de redundancia o una condición de recuperación.

Administración de la alimentación tras una falla de la unidad de suministro de energía

Cuando se produce un suceso de falta de alimentación, como una falla en una unidad de suministro de energía, el CMC reduce el suministro de energía a los servidores. Una vez reducido el suministro, el CMC reevalúa las necesidades de alimentación del chasis. Si aún no se cumplen los requisitos, el CMC apaga

los servidores de menor prioridad. No obstante, esto se hace en función de la política de redundancia de alimentación que haya establecido en el CMC. Un servidor redundante puede tolerar la pérdida de alimentación sin que se afecte el rendimiento de los servidores.

La alimentación a los servidores de mayor prioridad se restablece gradualmente, en tanto que las necesidades de alimentación se ajustan al presupuesto de alimentación. Para establecer la política de redundancia, consulte Configuración de la redundancia y el presupuesto de alimentación.

Administración de la alimentación tras la desconexión de una unidad de suministro de energía

Es posible que el CMC comience a conservar energía cuando se quita una unidad de suministro de energía o se quita el cable de CA de una unidad de suministro de energía. El CMC reduce la alimentación de los servidores con menor prioridad hasta que el consumo de energía pueda ser cubierto por las unidades de suministro de energía restantes en el chasis. Si quita más de una unidad de suministro de energía, el CMC volverá a evaluar las necesidades de alimentación al quitar la segunda unidad a fin de determinar la respuesta del firmware. Si aún no se cumplen los requisitos de alimentación, es posible que el CMC apague los servidores de menor prioridad.

Límites

- El CMC no admite el apagado *automatizado* de un servidor con menor prioridad para permitir el encendido de un servidor con mayor prioridad; sin embargo, se pueden realizar apagados iniciados por el usuario.
- Los cambios en la política de redundancia de las unidades de suministro de energía están limitados por el número de unidades de suministro de energía en el chasis. Se puede seleccionar cualquiera de los dos valores de configuración de la redundancia de las unidades de suministro de energía que se citan en Configuración de redundancia predeterminada.

Política de conexión de servidores nuevos

Si un servidor nuevo que se enciende excede la alimentación disponible para el chasis, el CMC puede disminuir la alimentación a los servidores de baja prioridad. Esto podría ocurrir si el administrador ha configurado un límite de alimentación para el chasis que está por debajo de lo que se requeriría para la asignación de alimentación total a los servidores, o si hay alimentación insuficiente disponible en caso de que los servidores en el chasis demanden requisitos de mayor alimentación. En caso de que no se pueda liberar suficiente alimentación al reducir la alimentación asignada de los servidores de prioridad baja, no se permite que el servidor nuevo se encienda.

Esto ocurre si el administrador había configurado un límite de alimentación para el chasis inferior a la asignación de alimentación total a los servidores o si la alimentación insuficiente está disponible para los servidores que requieren mayor alimentación.

En la siguiente tabla se describen las acciones realizadas por el CMC cuando se enciende un nuevo servidor en las condiciones descritas anteriormente.

Tabla 29. Respuesta del CMC cuando se intenta encender un servidor

Se cuenta con alimentación para el peor de los casos	Respuesta del CMC	Encendido del servidor
Sí	No se requiere la conservación de energía	Permitido
No	Se ejecuta la conservación de energía:	

Se cuenta con alimentación para el peor de los casos	Respuesta del CMC	Encendido del servidor
	• La alimentación requerida para el nuevo servidor está disponible	Permitido
	• La alimentación requerida para el nuevo servidor no está disponible	No permitido

Si una unidad de suministro de energía deja de funcionar, se produce un estado no crítico y se genera un suceso de falla de unidad de suministro de energía. Al desmontar una unidad de suministro de energía se genera un suceso de desmontaje de una unidad de suministro de energía.

Si uno de los sucesos ocasiona una pérdida de redundancia, en función de las asignaciones de alimentación, se genera un suceso de *pérdida de redundancia*.

Si la capacidad de alimentación posterior o la capacidad de alimentación del usuario es mayor que las asignaciones de los servidores, el rendimiento de los servidores se verá degradado o, en el peor de los casos, los servidores pueden llegar a apagarse. Ambas condiciones se dan en orden de prioridad inverso, es decir, los servidores de menor prioridad se apagan primero.

En la siguiente tabla se describe la respuesta del firmware ante el apagado o el desmontaje de una unidad de suministro de energía conforme se aplica a diversas configuraciones de redundancia de las unidades de suministro de energía.

Tabla 30. Impacto en el chasis de la falla o el desmontaje de una unidad de suministro de energía

Configuración de unidades de suministro de energía	Acoplamiento dinámico de unidades de suministro de energía	Respuesta del firmware
Redundancia de cuadrícula	Desactivado	El CMC envía alertas acerca de la pérdida de redundancia de cuadrícula.
Redundancia del suministro de energía	Desactivado	El CMC envía alertas acerca de la pérdida de redundancia del suministro de alimentación.
Redundancia de cuadrícula	Activado	El CMC le envía alertas acerca de la pérdida de redundancia de cuadrícula. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el desmontaje de una unidad de suministro de energía.
Redundancia del suministro de energía	Activado	El CMC informa al usuario que hay pérdida de redundancia de suministro de energía. Las unidades de suministro de energía en modo de espera (si existen) se encienden para compensar la pérdida del presupuesto de alimentación provocada por la falla o el desmontaje de una unidad de suministro de energía.

Cambios de suministro de energía y política de redundancia en el registro de sucesos del sistema

Los cambios en el estado de suministro de energía y en la política de redundancia de la alimentación se registran como sucesos. Los sucesos relacionados con el suministro de energía que registran anotaciones en el registro de sucesos del sistema (SEL) son inserción y extracción de suministros de energía, inserción y extracción de entrada de suministros de energía, y declaración y retiro de declaración de salida de suministros de energía.

La siguiente tabla incluye las anotaciones en el SEL que están relacionadas con los cambios en el suministro de energía:

Tabla 31. Sucesos del SEL para cambios de suministros de energía

Suceso de suministro de energía	Anotación del registro de sucesos del sistema (SEL)
Inserción	Hay suministro de energía.
Extracción	Falta el suministro de energía.
Entrada de CA recibida	Se ha restablecido la entrada de corriente del suministro de energía.
Entrada de CA perdida	Se ha perdido la entrada de corriente del suministro de energía <número>.
Salida de CC producida	El suministro de energía funciona normalmente.
Salida de CC perdida	Falló el suministro de energía.

Los sucesos relacionados con cambios en el estado de redundancia de alimentación que registran anotaciones en el SEL son la pérdida de redundancia y la recuperación de redundancia para el gabinete modular que está configurado para una política de alimentación de **Redundancia de la red eléctrica** o para una política de **Redundancia de suministro de energía**. La lista a continuación muestra las anotaciones del SEL relacionadas con los cambios en la política de alimentación de redundancia.

Suceso de política de alimentación	Anotación del registro de sucesos del sistema (SEL)
Redundancia perdida	Se ha perdido la redundancia de la fuente de alimentación.
Redundancia recuperada	The power supplies are redundant. (Las fuentes de alimentación son redundantes).

Configuración de la redundancia y el presupuesto de alimentación

Use esta página para configurar el presupuesto de alimentación, la redundancia y la alimentación dinámica de todo el chasis (chasis, servidores, módulos de E/S, KVM, CMC y suministros de energía), el cual utiliza cuatro unidades de suministro de energía (PSU). El servicio de administración de alimentación optimiza el consumo de energía y reasigna la alimentación a los distintos módulos según los requisitos.

Puede configurar los siguientes atributos:

- Límite de alimentación de entrada del sistema
- Política de redundancia

- Activar conexión dinámica del suministro de energía
- Desactivar botón de encendido del chasis
- Modo de conservación máx. de alimentación
- Registro remoto de la alimentación
- Intervalo del registro remoto de la alimentación
- Administración de la alimentación basada en servidor

Conservación de la energía y 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 del 1 al 9 a cada uno. El nivel de prioridad predeterminado para todos los servidores es 1. Cuanto menor es el número, mayor es el nivel de prioridad.

El presupuesto de alimentación se limita al máximo de cualquier grupo de dos unidades de suministro de energía que sea el más débil. Si intenta establecer un valor de presupuesto de alimentación de CA que exceda el valor de *Límite de alimentación de entrada del sistema*, el CMC mostrará un mensaje. El presupuesto de alimentación se limita a 4800 vatios.

Modo de conservación máxima de energía

Esto se activa para los modos Redundancia de cuadrícula o Redundancia de unidad de suministro de energía. El CMC realiza una conservación máxima de energía en los siguientes casos:

- El modo de conservación máxima está activado.
- Una secuencia de línea de comandos automatizada emitida por una fuente de alimentación ininterrumpible activa el modo de conservación máxima.

En el modo de conservación máxima, todos los servidores comienzan a funcionar a su nivel mínimo de energía y todas las solicitudes de asignación de energía del servidor se rechazan. En este modo, el rendimiento de los servidores encendidos puede degradarse. Los servidores adicionales no pueden encenderse, independientemente de la prioridad del servidor.

El sistema se restablece al rendimiento óptimo cuando se desactiva el modo de conservación máxima.

Reducción de la alimentación del servidor para mantener el presupuesto de alimentación

El CMC reduce la asignación de alimentación a los servidores de menor prioridad cuando se necesita energía adicional para mantener el consumo de alimentación del sistema dentro del valor de *Límite de alimentación de entrada del sistema*. Por ejemplo, cuando se conecta un nuevo servidor, el CMC podría reducir la alimentación de los servidores de menor prioridad para obtener más alimentación para el

servidor nuevo. Si después de reducir la asignación de alimentación a los servidores de menor prioridad la cantidad de energía aún no es suficiente, el CMC disminuirá el rendimiento de los servidores hasta liberar suficiente energía para alimentar el servidor nuevo.

El CMC reduce la asignación de alimentación a los servidores en dos casos:

- El consumo general de alimentación excede el valor de *Límite de alimentación de entrada del sistema*.
- Se produce una falla de alimentación en una configuración sin redundancia.

Operación de unidades de suministro de energía de 110 V

De forma predeterminada, está disponible la función Operación de CA de la unidad de suministro de energía a 110 V. Sin embargo, no se admite la combinación de operación a 110 V y 220 V. Si el CMC detecta que ambos voltajes son de entrada, se selecciona un valor de voltaje y se desactivan esos suministros de energía conectados al otro nivel de voltaje, y se indican como fuera de funcionamiento.

Registro remoto

Se puede informar sobre el consumo de alimentación a un servidor syslog remoto. Es posible registrar información sobre el consumo total del chasis, el consumo de alimentación mínimo, máximo y medio en un período de recopilación. Para obtener más información sobre la manera de activar esta función y configurar el intervalo de recopilación y registro, consulte Administración y supervisión de energía.

Administración de la alimentación externa

La administración de la alimentación del CMC se controla opcionalmente mediante OpenManage Power Center (OMPC). Para obtener más información, consulte la *Guía del usuario de OMPC*.

Si está activada la administración de la alimentación externa, OMPC administra lo siguiente:

- Alimentación de servidores VRTX compatibles
- Alimentación de servidores VRTX compatibles
- Capacidad de alimentación de entrada del sistema
- Modo de conservación máxima de energía

El CMC sigue manteniendo o administrando lo siguiente:

- Política de redundancia
- Registro remoto de la alimentación
- Rendimiento del sistema sobre redundancia de alimentación
- Conexión dinámica de suministros de energía

OMPC administra la priorización y la alimentación de los nodos de servidores VRTX en el chasis con el presupuesto disponible tras la asignación de alimentación a la infraestructura de chasis y los nodos de servidores de generaciones anteriores. El registro remoto de la alimentación no se ve afectado por la administración de la alimentación externa.

Una vez que se haya activado el modo de administración de la alimentación basada en servidor, el chasis estará preparado para la administración de la PM3. La prioridad de todos los servidores VRTX se define en 1 (Alta). La PM3 administra las prioridades y la alimentación de los servidores directamente. La PM3

controla las asignaciones de alimentación de servidores compatibles, por lo que el CMC ya no controla el modo de conservación máxima de energía y se desactiva esta selección.

Si se activa el **Modo de conservación máxima de energía**, el CMC establece la capacidad de alimentación de entrada del sistema en el máximo que admite el chasis. El CMC no permite que la alimentación supere la capacidad máxima. Sin embargo, la PM3 administra todos los demás límites de capacidad de alimentación.

Si la administración de la alimentación de la PM3 está desactivada, el CMC vuelve a los valores de prioridad de los servidores configurados antes de que se activase la administración externa.

NOTA: Cuando la administración de la PM3 está desactivada, el CMC no vuelve a la configuración anterior de la alimentación máxima del chasis. Consulte el **registro del CMC** para conocer la configuración anterior y restaurar el valor manualmente.

Configuración de la redundancia y el presupuesto de alimentación mediante la interfaz web del CMC

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Para configurar el presupuesto de alimentación:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Alimentación → Configuración**.
2. En la página **Configuración de la redundancia/presupuesto**, seleccione alguna o todas las propiedades siguientes. Para obtener información sobre las descripciones de los campos, consulte la *Ayuda en línea*.
   - **Activar administración de la alimentación basada en servidor**
   - **Límite de alimentación de entrada del sistema**
   - **Política de redundancia**
   - **Activar conexión dinámica del suministro de energía**
   - **Desactivar botón de encendido del chasis**
   - **Modo de conservación máx. de alimentación**
   - **Activar registro de alimentación remoto**
   - **Intervalo del registro remoto de la alimentación**
3. Haga clic en **Aplicar** para guardar los cambios.

Configuración de la redundancia y el presupuesto de alimentación mediante RACADM

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Para activar la redundancia y establecer la política de redundancia:

1. Abra una consola de texto de serie/Telnet/SSH en el CMC e inicie sesión.
2. Establezca las propiedades según sea necesario:
   - Para seleccionar una política de redundancia, escriba:
     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <value>
     ```

donde <*value*> es 1 (redundancia de cuadrícula) y 2 (redundancia de suministro de energía). El valor predeterminado es 2.

Por ejemplo, el siguiente comando establece la política de redundancia en 1:

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
```

- Para establecer el valor del presupuesto de alimentación, escriba:
  ```
  racadm config -g cfgChassisPower -o cfgChassisPowerCap <valor>
  ```
  donde <*valor*> es un número entre 938 W y 4800 W, que representa el límite máximo de la alimentación en vatios. El valor predeterminado es 4800.
  Por ejemplo, el siguiente comando establece el presupuesto máximo de la alimentación en 4800 vatios:
  ```
  racadm config -g cfgChassisPower -o cfgChassisPowerCap 4800
  ```
- Para activar o desactivar la conexión dinámica de las unidades de suministro de energía, escriba:
  ```
  racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable
  <value>
  ```
  donde <*valor*> es 0 Usuarios locales (desactivar), 1 (activar). El valor predeterminado es 0.
  Por ejemplo, el siguiente comando desactiva el acoplamiento dinámico de unidades de suministro de energía:
  ```
  racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
  ```
- Para activar el modo de consumo máximo de alimentación, escriba:
  ```
  racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 1
  ```
- Para restaurar el funcionamiento normal, escriba:
  ```
  racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
  ```
- Para activar la función de registro remoto de alimentación, introduzca el comando siguiente:
  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
  ```
- Para especificar el intervalo de registro deseado, introduzca el comando siguiente:
  ```
  racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval n
  ```
  donde *n* es un valor de 1 a 1.440 minutos.
- Para comprobar que la función de registro remoto de alimentación está activada, introduzca el comando siguiente:
  ```
  racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
  ```
- Para determinar el intervalo de registro remoto de alimentación, escriba el comando siguiente:
  ```
  racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
  ```
  La función de registro remoto de alimentación depende de que los host de syslog remoto se hayan configurado previamente. Se debe activar el registro a uno o varios host de syslog remoto; de lo contrario, se registrará el consumo de alimentación. Esto se puede realizar mediante la interfaz gráfica de usuario o la CLI de RACADM. Para obtener más información, consulte las instrucciones de configuración de syslog remoto.
- Para activar la administración de alimentación remota por Open Manage Power Center (OPMC), escriba:
  ```
  racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 1
  ```
- Para restaurar la administración de la alimentación del CMC, escriba lo siguiente:
  ```
  racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 0
  ```

Para obtener más información acerca de los comandos de RACADM para la alimentación del chasis, consulte las secciones **config**, **getconfig**, **getpbinfo** y **cfgChassisPower** de *Chassis Management*

Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de Chassis Management Controller para la línea de comandos RACADM de PowerEdge VRTX).

Ejecución de las operaciones de control de alimentación

Puede ejecutar la siguiente operación de control de alimentación para chasis, servidores y módulos de E/S.

NOTA: Las operaciones de control de alimentación afectan a todo el chasis.

Ejecución de operaciones de control de alimentación en el chasis

El CMC le permite realizar de manera remota varias acciones de administración de la alimentación, por ejemplo, un apagado ordenado, en todo el chasis (el chasis, los servidores, los módulos de E/S y las unidades de suministro de energía).

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de control del chasis**.

Ejecución de operaciones de control de alimentación en el chasis mediante la interfaz web

Para ejecutar operaciones de control de alimentación en el chasis mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción del chasis** → **Alimentación** → **Control**.
   Aparecerá la página **Control de alimentación del chasis**.
2. Seleccione una de las siguientes operaciones de control de alimentación.
   Para obtener información sobre cada opción, consulte la *Ayuda en línea*.
   - **Encender el sistema**
   - **Apagar el sistema**
   - **Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)**
   - **Restablecer el CMC (reinicio mediante sistema operativo)**
   - **Apagado no ordenado**
3. Haga clic en **Apply (Aplicar)**.
   Aparecerá un cuadro de diálogo que solicita confirmación.
4. Haga clic en **Aceptar** para realizar la acción de administración de la alimentación (por ejemplo, hacer que se restablezca el sistema).

Ejecución de operaciones de control de alimentación en el chasis mediante RACADM

Abra una consola de texto de serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm chassisaction -m chassis <action>
```

donde <*action*> es powerup, powerdown, powercycle, nongraceshutdown o reset.

Ejecución de operaciones de control de alimentación en un servidor

Es posible realizar acciones de administración de alimentación de forma remota para varios servidores a la vez o un servidor individual en el chasis.

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Ejecución de operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC

Para ejecutar operaciones de control de alimentación para varios servidores mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del servidor → Alimentación**.
   Aparecerá la página **Control de alimentación**.
2. En la columna **Operaciones**, en el menú desplegable, seleccione una de las siguientes operaciones de control de alimentación para los servidores requeridos:
   - **Sin operación**
   - **Encender el servidor**
   - **Apagar el servidor**
   - **Apagado ordenado**
   - **Restablecer el servidor (reinicio mediante sistema operativo)**
   - **Ciclo de encendido del servidor (reinicio mediante suministro de energía)**

   Para obtener más información acerca de estas opciones, consulte la *Ayuda en línea*.
3. Haga clic en **Apply (Aplicar)**.
   Aparecerá un cuadro de diálogo que solicita confirmación.
4. Haga clic en **Aceptar** para ejecutar la acción de administración de alimentación (por ejemplo, restablecer el servidor).

Ejecución de operaciones de control de alimentación en el módulo de E/S

Es posible restablecer o encender de forma remota un módulo de E/S.

NOTA: Para realizar acciones de administración de alimentación, debe contar con privilegios de **Administrador de configuración del chasis**.

Ejecución de operaciones de control de alimentación en módulos de E/S mediante la interfaz web del CMC

Para ejecutar operaciones de control de alimentación en el módulo de E/S:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Descripción general del módulo de E/S → Alimentación**.
2. Para el módulo de E/S, en la página **Control de alimentación** seleccione desde el menú desplegable la operación que desea ejecutar (ciclo de encendido).

3. Haga clic en **Apply (Aplicar)**.

Ejecución de operaciones de control de alimentación en el módulo de E/S mediante RACADM

Para ejecutar operaciones de control de alimentación en el módulo de E/S mediante RACADM, abra una consola de texto de serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm chassisaction -m switch <action>
```

en donde <*action*> indica la operación que desea ejecutar: ciclo de encendido.

15

Administración del almacenamiento del chasis

En Dell PowerEdge VRTX, es posible realizar las siguientes operaciones:

- Ver el estado de las unidades de discos físicos y controladoras de almacenamiento.
- Ver las propiedades de las controladoras, las unidades de discos físicos, los discos virtuales y los gabinetes.
- Configurar controladoras, unidades de discos físicos y discos virtuales.
- Asignar adaptadores virtuales.
- Solucionar problemas en controladoras, unidades de discos físicos y discos virtuales.
- Actualizar componentes de almacenamiento.
- Usar las controladoras de almacenamiento compartido en modo con tolerancia a errores
- Activación o desactivación de PERC8 compartido (integrado 2)

Visualización del estado de los componentes de almacenamiento

Para ver el estado de los componentes de almacenamiento:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Propiedades** → **Descripción general del almacenamiento**.
2. En la página **Descripción general del almacenamiento**, es posible:
   - Ver el resumen gráfico de las unidades de discos físicos instaladas en el chasis y su estado.
   - Ver el resumen de todos los componentes de almacenamiento con enlaces a sus respectivas páginas.
   - Ver la capacidad utilizada y la capacidad total del almacenamiento.
   - Ver información de la controladora.

     NOTA: En el caso de una controladora con tolerancia a errores, el formato de nombre es: Shared <*número de PERC*> (integrada<número>). Por ejemplo, la controladora activa es Shared PERC8 (integrada 1) y la controladora homóloga es Shared PERC8 (integrada 2).

     NOTA: Si la controladora PERC está desactivada, el nombre se muestra como **PERC desactivada (integrada 2)**.
   - Ver los sucesos de almacenamiento registrados recientemente.

   NOTA: Para obtener más información, consulte la *ayuda en línea*.

Visualización de la topología de almacenamiento

Para ver la topología de almacenamiento:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Almacenamiento → Propiedades → Topología**.
2. En la página **Topología**, haga clic en el **<nombre de la controladora>** para ver las páginas correspondientes.

   NOTA: Puede ver el nombre de la controladora que está activa al controlar los dispositivos de almacenamiento asociados con este CMC y también la controladora pasiva que actúa como controladora en espera.
3. En cada controladora instalada, haga clic en los vínculos **Ver discos virtuales**, **<nombre del gabinete>** y **Ver discos físicos** para abrir las páginas correspondientes.

Visualización de la información de solución de problemas con tolerancia a errores de SPERC mediante la interfaz web del CMC

Para ver los atributos que indican el correcto funcionamiento de las funciones con tolerancia a errores de una SPERC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Almacenamiento → Solución de problemas → Solución de problemas de configuración**.

   Aparece la página **Solución de problemas de configuración del almacenamiento**.
2. En la página **Solución de problemas de configuración del almacenamiento**, puede:
   - Ver los siguientes atributos cuando la controladora está en modo con tolerancia a errores:
     - Dos PERC compartidas detectadas.
     - Dos expansores detectados
     - PERC compartidas y expansores cableados correctamente
     - Firmware correcto en las PERC compartidas
     - Firmware correcto en los expansores
     - Firmware correcto en la infraestructura del chasis
     - Las PERC compartidas tienen los mismos valores: indica si las SPERC tienen los mismos valores o no.
   - Vea los siguientes atributos cuando la controladora no está en el modo con tolerancia a errores:
     - Una PERC compartida detectada.
     - Un expansor detectado
     - PERC compartida y expansores cableados correctamente
   - Vea el estado de cada atributo que indica si se ha cumplido con los criterios de la tolerancia a errores.

     NOTA: Si el atributo del entorno con tolerancia a errores no coincide con el criterio, aparece la opción **Actualizar ahora** para ese atributo.

   NOTA: Aparece la opción **Más información** para algunos de los atributos. Para obtener más información sobre el atributo, haga clic en **Más información**.

3. Para cumplir con el criterio de un atributo, haga clic en **Actualizar ahora**.

   Aparece la página **Actualización del componente de almacenamiento**, que le permite actualizar el componente de almacenamiento requerido para cumplir con el criterio del atributo.

Asignación de adaptadores virtuales para ranuras mediante la interfaz web del CMC

Si usa la función Adaptador virtual, puede compartir el almacenamiento instalado con los cuatro servidores. Para asignar un disco virtual a una ranura de servidor, primero debe asignar un disco virtual a un adaptador virtual (VA) y, a continuación, un adaptador virtual (VA) a una ranura de servidor.

- Antes de asignar un adaptador virtual a una ranura de servidor, asegúrese de lo siguiente:
  - La ranura del servidor debe estar vacía o el servidor de esa ranura debe estar apagado.
  - Se desasignó el adaptador virtual de un servidor o de una ranura.
  - Todos los servidores afectados están apagados.
- Los discos virtuales se crean y se asignan como **Adaptador virtual 1**, **Adaptador virtual 2**, **Adaptador virtual 3** o **Adaptador virtual 4**. Para obtener más información, consulte la sección Aplicación de la política de acceso de adaptadores virtuales a discos virtuales.

NOTA:

- Puede asignar únicamente un adaptador virtual a un servidor a la vez.
- Sin una licencia adecuada, puede desasignar solo una asignación de adaptador virtual-servidor o asignar el adaptador virtual al servidor predeterminado.
- La asignación predeterminada es adaptador virtual 1-ranura de servidor 1, adaptador virtual 2-ranura de servidor 2, adaptador virtual 3-ranura de servidor 3 y adaptador virtual 4-ranura de servidor 4.
- Si se inserta un servidor de altura completa, la ranura superior tiene el adaptador virtual asignado mientras que la ranura inferior aún está sin asignar. Por ejemplo, un servidor de altura completa en la ranura 1 tiene el adaptador virtual 1 asignado a la ranura 1 y el adaptador virtual 3 sin asignar.
- Si el sistema tiene una licencia Enterprise, puede asignar cualquiera de los cuatro adaptadores virtuales a una ranura de servidor. Sin embargo, aún puede asignar un adaptador virtual a un servidor a la vez.

Para asignar o desasignar un adaptador virtual de una ranura de servidor:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Configuración** → **Virtualización**.

   Aparece la página **Virtualización del almacenamiento**.
2. Para seleccionar el tipo de asignación necesario, desde la tabla **Modo de asignación: discos virtuales a adaptadores virtuales**, seleccione:
   - **Asignación individual**: seleccione esta opción para asignar un disco virtual a un adaptador virtual.
   - **Asignación múltiple**: seleccione esta opción para asignarle un disco virtual a varios adaptadores virtuales. Lea las instrucciones en pantalla antes de seleccionar esta opción.

   NOTA: Seleccione el modo **Asignación múltiple** solo cuando los servidores tienen los servicios de clúster instalado. El uso de este modo sin los servicios de clúster puede provocar una pérdida de datos o dañarlos.
3. En la tabla **Adaptadores virtuales asignados**, en el menú desplegable **Acción**, seleccione una de las siguientes opciones y, a continuación, haga clic en **Aplicar**.

- **<N° ranura>**: seleccione la ranura a la que se le debe asignar el adaptador virtual.
- **Desasignar**: seleccione esta opción para eliminar la asignación del adaptador virtual a una ranura.

El adaptador virtual se asigna o desasigna de la ranura de servidor seleccionada según la acción seleccionada.

NOTA: Tenga en cuenta un adaptador virtual asignado al servidor en la ranura inferior (3 o 4). Cuando se reemplaza un servidor de mitad de altura (ranura 3 o 4) por un servidor de altura completa, este último no accede al adaptador virtual asignado a las ranuras inferiores. Si inserta un servidor de mitad de altura de nuevo, se puede acceder al adaptador virtual.

Tolerancia a errores en las controladoras de almacenamiento

La alta disponibilidad (HA) de almacenamiento permite la disponibilidad de varios componentes internos y varios puntos de acceso a los recursos de almacenamiento. Si un componente de almacenamiento deja de funcionar, el servidor es admitido por un segundo componente crítico o por la ruta de acceso a los datos disponibles. La alta disponibilidad solamente minimiza el tiempo de inactividad ya que restaura servicios tras bambalinas, en la mayoría de los casos antes de que la no funcionalidad sea visible, pero no elimina el tiempo de inactividad. La tolerancia a errores (FT) utiliza componentes redundantes dentro de un sistema de almacenamiento que están configurados para actuar como componentes de copia de seguridad y se mantienen en modo de espera. Las controladoras de almacenamiento en modo con tolerancia a errores evitan la interrupción de los servicios de almacenamiento y toman automáticamente los servicios del componente que ha dejado de funcionar. El rendimiento sigue siendo constante a través de este proceso de conmutación por error dado que los componentes redundantes (controladoras) no se usan durante condiciones normales de funcionamiento.

La alta disponibilidad con tolerancia a errores ofrece los siguientes beneficios:

- Proporciona tiempo de actividad para todas las aplicaciones de almacenamiento incluso cuando una controladora deja de funcionar.
- Proporciona acceso a funciones críticas del chasis en todo momento.
- Activa el servidor para manejar situaciones de falla cuando la controladora deja de funcionar.
- Usa la redundancia de los componentes

Si utiliza la función de tolerancia a errores de las controladoras, puede administrar las tareas asociadas con el almacenamiento compartido que se consiguen al tener una controladora activa y pasiva (homóloga). La controladora activa es la controladora que supervisa todos los procesos relacionados con el almacenamiento. El estado de funcionamiento de ambas controladoras se comunica entre las controladoras de modo que cuando la controladora activa deja de funcionar, la controladora pasiva actúa como repuesto dinámico homólogo, es decir, toma el control sin problemas.

NOTA: El CMC muestra datos de la tolerancia a errores de Shared PERC 8 con firmware activado SR-IOV. Si hay una tarjeta no perteneciente a SR-IOV conectada a las ranuras de almacenamiento compartido, la tarjeta no se enciende y se genera una alerta.

Visualización de las propiedades de la controladora mediante la interfaz web del CMC

Para ver las propiedades de la controladora:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Controladora**.
2. En la página **Controladoras**, en la sección **Controladoras**, es posible ver las propiedades básicas de la controladora. Sin embargo, para ver las propiedades avanzadas, haga clic en el +.

   NOTA: Si las controladoras están en modo con tolerancia a errores, también aparece la siguiente información sobre el estado y el modo de la tolerancia a errores:

   - Modo con tolerancia a errores: compartido, activo/pasivo
   - Estado con tolerancia a errores: satisfactorio/normal o perdido/degradado
   - Controladora homóloga: indica el nombre de la controladora que actúa como homóloga (en espera) en el caso de un modo con tolerancia a errores admitido por dos controladoras.

   NOTA: Si la controladora homóloga está desactivada, el nombre se muestra como **PERC desactivada (integrada 2)** y el estado aparecerá como **Desconocido**, lo que implica que la controladora homóloga está apagada.

   Para obtener más información acerca de las controladoras, consulte la *Ayuda en línea*.

Visualización de las propiedades de las controladoras mediante RACADM

Para ver las propiedades de las controladoras mediante RACADM, ejecute el comando `racadm raid get controllers -o`

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX).

Importación o borrado de configuración ajena

Debe insertarse un disco ajeno en el chasis.
Para importar o borrar la configuración ajena:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Controladoras** → **Configuración**.
2. En la página **Configuración de la controladora**, en la sección **Configuración ajena**, para la controladora correspondiente haga clic en:
   - **Borrar configuración ajena** para borrar la configuración actual del disco.
   - **Importar/Recuperar** para importar el disco con la configuración ajena.

Configuración de los valores de la controladora de almacenamiento

Puede modificar las propiedades existentes de una controladora de almacenamiento o configurar las propiedades de una controladora de almacenamiento recién instalada.

Configuración de los valores de la controladora de almacenamiento mediante la interfaz web del CMC

Asegúrese de que haya al menos una controladora de almacenamiento instalada en el chasis. Para configurar los valores de la controladora de almacenamiento:

1. En la interfaz web del CMC, vaya a **Descripción general del chasis** → **Almacenamiento** → **Controladoras** → **Configuración**.
2. En la página **Configuración de la controladora**, desde el menú desplegable **Controladora**, seleccione la controladora.

   NOTA: Tenga en cuenta lo siguiente:

   - Si las controladoras de almacenamiento están en modo con tolerancia a errores y si ambas tienen la misma versión de firmware, las dos aparecen como un solo dispositivo en el menú desplegable. Por ejemplo, Shared PERC8 (integrada 1)/Shared PERC8 (integrada 2). Si la configuración de las dos controladoras es diferente, aparece el mensaje **Configuración incompatible**. Puede establecer las propiedades de las controladoras con tolerancia a errores para que dichas propiedades sean las mismas en ambas controladoras. En este modo, las controladoras no pueden tener propiedades distintas.
   - Si se instala una segunda controladora de almacenamiento con otra versión de firmware, las controladoras aparecen como dos componentes distintos en el menú desplegable. Por ejemplo, Shared PERC8 (integrada 1) y Shared PERC8 (integrada 2).

   Los valores de atributos para la controladora seleccionada se actualizan en la tabla.
3. Escriba o seleccione los datos adecuados y, a continuación, haga clic en **Aplicar**.

   NOTA: Para obtener información sobre los atributos y las descripciones de otros campos, consulte la *Ayuda en línea*.

   Las propiedades configuradas recientemente se aplican a las controladoras seleccionadas y el campo **Valor actual** muestra los valores actualizados para los atributos.

Configuración de los valores de la controladora de almacenamiento mediante RACADM

Para configurar la controladora de almacenamiento mediante la ejecución de un comando de RACADM, utilice la sintaxis siguiente.

```
racadm raid ctrlprop:RAID.ChassisIntegrated.1-1 [-rebuild <value>] [-bgi
<value>] [-reconstruct <value>] [-checkconsistency <value>] [-ccmode
{abortonerror | normal}] [-copybackmode {off | on | onwithsmart}] [-lb {auto |
disabled}] [-prunconfigured {yes | no}]
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Controladoras PERC compartidas

Para los sistemas VRTX enviados con dos controladoras PERC, la segunda controladora PERC es posible que se haya desactivado. En este modo el chasis no funciona en el modo Tolerancia de errores. Luego, el sistema funciona como un solo sistema PERC compartido con una sola controladora activa que funciona en modo **Performance** (Rendimiento).

Desde la interfaz de línea de comandos de RACADM, ejecute el comando`racadm raid get controllers` para generar una lista con el número de controladoras PERC compartidas en el sistema. Si el comando enumera solamente `RAID.ChassisIntegrated.1-1`, el sistema tiene una única controladora PERC compartida. Si el comando enumera `RAID.ChassisIntegrated.1-1`y `RAID.ChassisIntegrated.2-1`, el sistema dispone de dos controladoras PERC compartidas.

Para los sistemas con dos controladoras PERC compartidas instaladas, puede cambiar el modo de funcionamiento desde el modo de **Rendimiento** al modo de **Tolerancia de errores**, o a través de la interfaz web o la CLI de RACADM.

Para cambiar el modo de funcionamiento mediante la interfaz web del CMC, vaya a la página **Controladoras Solución de problemas** ; para ello, vaya a **Descripción general del chasis** → **Controladoras de almacenamiento** en el panel izquierdo y seleccione la opción **Disable Raid Controller** o **Enable Raid Controller**.

Para cambiar el modo de funcionamiento mediante la CLI de RACADM:

- Ejecute el comando `racadm raid enableperc:RAID.ChassisIntegrated.2-1` para seleccionar el modo **PERC compartido con tolerancia a fallas** .
- Ejecute el comando `racadm raid disableperc:RAID.ChassisIntegrated.2-1` para seleccionar el modo **Rendimiento**.

NOTA: El chasis debe estar encendido y todos los módulos del servidor deben estar apagados antes de ejecutar los comandos de activar o desactivar. El chasis pasa automáticamente por un ciclo de alimentación como parte de esta operación. Después de cambiar el modo de funcionamiento de la PERC compartido, es recomendable restablecer el CMC por medio de la página **Resolución de problemas** o el comando `racadm racreset`.

Activación o desactivación de alertas mediante la interfaz web del CMC

Para un chasis VRTX con dos controladoras PERC8 compartidas, el adaptador PERC integrado 2 se puede desactivar o activar cuando el adaptador PERC integrado 1 esté activa y todos los módulos de servidor se encuentren apagados. Ambos adaptadores deben estar habilitados para la tolerancia a errores. La página **Solución de problemas de controladoras** le permite activar o desactivar la controladora homóloga.

NOTA: Para evitar la pérdida de datos, antes de realizar operaciones de activación o desactivación de la controladora:

- Complete todas las operaciones de datos como Reconstrucción o Volver a copiar.
- Asegúrese de que los volúmenes de datos se encuentren en estado óptimo.

NOTA: Al activar el segundo adaptador PERC, aparecerá un mensaje de advertencia y el estado de tolerancia a fallas se degrada si:

- Se cambia cualquiera de los valores del adaptador PERC.
- Se actualiza el firmware.

Asegúrese de que el firmware y la configuración del PERC compartido coincidan a fin de establecer la configuración de tolerancia a fallas en el modo de tolerancia a fallas.

Puede desactivar una controladora homóloga únicamente si:

- Se apagan todos los servidores que están en el chasis.

- La PERC 1 integrada es actualmente la controladora activa.

  NOTA: Si la PERC 1 integrada actualmente no es la controladora activa, realice un ciclo de encendido del chasis para hacer que sea la controladora activa.

- Ambos CMC tienen la misma versión de firmware que admite esta función.

NOTA: Después de desactivar el PERC integrado 2, en caso de tener que sustituir una tarjeta del CMC, se recomienda actualizar la tarjeta del CMC con el firmware de versión 1.35 o posterior, antes de asignar la tarjeta para que sea la controladora CMC activa en el sistema. Aparece un mensaje de aviso antes de llevar a cabo esta acción.

Para activar o desactivar una controladora homóloga en modo de tolerancia a fallas mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Almacenamiento → Controladoras → Solución de problemas**.
2. En la página **Solución de problemas de la controladora**, en el menú desplegable **Acciones** para PERC integrado 2, seleccione una de las siguientes opciones y haga clic en **Aplicar**.
   - **Desactivar controladora RAID**: desactiva la controladora homóloga en el modo con tolerancia a fallas. Esta opción está disponible solamente en el menú desplegable para PERC integrado 2 cuando no está desactivado.
   - **Activar controladora RAID**: activa la controladora homóloga en el modo con tolerancia a fallas. Si PERC integrado 2 ya está desactivado, la opción **Activar controladora RAID** está disponible en el menú desplegable.

     NOTA: En el caso de que PERC esté desactivado, ninguna de las demás opciones Restablecer configuración, Exportar registro de TTY, Descartar memoria caché anclada y Desactivar controladora RAID está disponibles en el menú desplegable.

NOTA: Al activar o desactivar una controladora homóloga, se inicia un ciclo de encendido del chasis. Los cambios se reflejarán solo después de que se complete el ciclo de encendido.

Activación o desactivación de la controladora RAID mediante RACADM

Para activar una controladora homóloga mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm raid enableperc:<AdapterFQDD>
```

Para desactivar una controladora homóloga, introduzca:

```
racadm raid disableperc:<AdapterFQDD>
```

NOTA: Para obtener más información sobre esta función mediante la interfaz de RACADM, consulte *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de línea de comandos de RACADM para iDRAC y CMC).

Visualización de las propiedades del disco físico mediante la interfaz web del CMC

Asegúrese de que los discos físicos estén instalados en el chasis.
Para ver las propiedades de las unidades de disco físico:

1. En el panel izquierdo, vaya a **Descripción general del chasis → Almacenamiento → Discos físicos**.

Aparecerá la página **Propiedades**.

2. Para ver las propiedades de todas las unidades de disco físico, en la sección **Disco físico** haga clic en el .

   NOTA: Para el modo con tolerancia a errores, también aparecen los siguientes atributos:

   - Controladora activa: Shared PERC8 (integrada 1)
   - Controladora redundante/contra fallas: Shared PERC8 (integrada 2)

   También puede utilizar los siguientes filtros para ver las propiedades de unidades de disco físico específicas:

   - En la opción **Filtro básico de discos físicos** del menú desplegable **Agrupar por**, seleccione **Disco virtual**, **Controladora** o **Gabinete**, y luego haga clic en **Aplicar**.
   - Haga clic en **Filtro avanzado**, seleccione los valores de los diversos atributos y luego haga clic en **Aplicar**.

Visualización de propiedades de unidades de discos físicos mediante RACADM

Para ver las propiedades de las unidades de discos físicos mediante RACADM, ejecute el comando `racadm raid get pdisks –o`

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Identificación de discos físicos y discos virtuales

Para obtener más información acerca de cómo activar o desactivar la función de parpadeo de LED, consulte:

- Configuración del parpadeo de LED mediante la interfaz web del CMC
- Configuración del parpadeo de LED a través de RACADM

Asignación de repuestos dinámicos globales mediante la interfaz web del CMC

Para asignar o desasignar un repuesto dinámico global:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Disco físico** → **Configuración**.

   Se mostrará la página **Configurar discos físicos**.

2. En la sección **Asignación de repuestos dinámicos globales** del menú desplegable **Acción del repuesto dinámico**, seleccione **Desasignar** o **Repuesto dinámico global** para cada una de las unidades de disco físico y luego haga clic en **Aplicar**. O bien, desde el menú desplegable **Acción del repuesto dinámico: Asignar a todos**, seleccione **Desasignado** o **Repuesto dinámico global** y luego haga clic en **Aplicar**.

Asignación de repuestos dinámicos globales mediante RACADM

Para asignar un repuesto dinámico global mediante RACADM, ejecute el comando `racadm raid hotspare: -assign yes -type ghs`.

Para obtener más información sobre cómo usar comandos RACADM, consulte la *Guía de referencia sobre líneas de comando RACADM de Chassis Management Controller para PowerEdge VRTX*.

Recuperación de discos físicos

Para recuperar un disco físico:

1. En la interfaz web del CMC, vaya a **Descripción general del chasis** → **Almacenamiento** → **Discos físicos** → **Configuración**.
2. En la página **Configuración**, bajo la sección **Recuperar discos físicos**, seleccione el disco físico que se debe recuperar y desde el menú desplegable, seleccione **Recrear unidad**, **Cancelar recreación** o **Forzar en línea** según corresponda y, a continuación, haga clic en **Aplicar**.

Visualización de propiedades de discos virtuales mediante la interfaz web del CMC

Asegúrese de que se hayan creado discos virtuales.
Para ver las propiedades de los discos virtuales:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Discos virtuales** → **Propiedades**.
2. En la página **Propiedades**, de la sección **Discos virtuales**, haga clic en el . También puede utilizar los siguientes filtros para ver propiedades específicas de los discos virtuales:
   - En la sección **Filtro básico de discos virtuales** del menú desplegable **Controladora**, seleccione el nombre de la controladora y luego haga clic en **Aplicar**.
   - Haga clic en **Filtro avanzado**, seleccione los valores de los diversos atributos y luego haga clic en **Aplicar**.

Visualización de propiedades de discos virtuales mediante RACADM

Para ver las propiedades de un disco virtual mediante RACADM, ejecute el comando `racadm raid get vdisks -o`

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Creación de un disco virtual mediante la interfaz web del CMC

Asegúrese de que el disco físico esté instalado en el chasis.

NOTA: Al eliminar un disco virtual, se quita el disco virtual de la configuración de la controladora.

Para crear un disco virtual:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Almacenamiento → Discos virtuales → Crear**.
2. En la página **Crear un disco virtual**, en la sección **Configuración**, escriba los datos adecuados, y en la sección **Seleccionar discos físicos**, seleccione la cantidad de unidades de discos físicos en función del nivel RAID seleccionado anteriormente y, a continuación, haga clic en **Crear un disco virtual**.

Aplicación de la política de acceso para adaptadores virtuales a discos virtuales

Asegúrese de que las unidades de discos físicos estén instaladas y que se hayan creado discos virtuales. Para aplicar la política de acceso para adaptadores virtuales:

1. En el panel izquierdo, haga clic en **Descripción del chasis → Almacenamiento → Discos virtuales → Asignar**.
2. En la página **Asignar discos virtuales**, en la sección **Política de acceso para adaptadores virtuales** del menú desplegable **Adaptador virtual <número>**, seleccione **Acceso total** para cada unidad de disco físico.
3. Haga clic en **Apply (Aplicar)**.

Ahora podrá asignar adaptadores virtuales a ranuras del servidor. Para obtener más información, consulte la sección Asignación de adaptadores virtuales a ranuras de esta Guía del usuario.

Modificación de las propiedades de disco virtual mediante la interfaz web del CMC

Para modificar las propiedades del disco virtual:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Almacenamiento → Discos virtuales → Administrar**.
2. En la página **Administrar discos virtuales**, en el menú desplegable **Acciones del disco virtual**, seleccione una de las siguientes acciones y, a continuación, haga clic en **Aplicar**.
   - **Cambiar nombre**
   - **Eliminar**

     NOTA: Si selecciona Eliminar, se muestra el siguiente mensaje que indica que la eliminación de un disco virtual eliminará de forma permanente los datos disponibles en dicho disco virtual.

     ```
     Deleting the virtual disk removes the virtual disk from the
     controller's configuration. Initializing the virtual disk permanently
     erases data from the virtual disk.
     ```

   - **Política de edición: Caché de lectura**
   - **Política de edición: Caché de escritura**
   - **Política de edición: Caché del disco**
   - **Inicialización: rápida**
   - **Inicialización: completa**

Visualización de las propiedades del gabinete mediante la interfaz web del CMC

Para ver las propiedades del gabinete:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Almacenamiento** → **Gabinetes** → **Propiedades**.
2. En la página **Propiedades**, en la sección **Gabinete**, haga clic en el  para obtener una visualización gráfica de las unidades de discos físicos y sus estados, un resumen de las ranuras de unidades de discos físicos y las propiedades avanzadas.

16

Administración de ranuras PCIe

Todas las ranuras están desasignadas de manera predeterminada. Puede hacer lo siguiente:

- Ver el estado de todas las ranuras PCIe del chasis.
- Asignar o quitar una ranura PCIe asignada de los servidores.

Tenga en cuenta lo siguiente antes de asignar una ranura PCIe a un servidor:

- Si una ranura PCIe está vacía, no se la puede asignar a un servidor encendido.
- Una ranura PCIe que tiene un adaptador asignado a un servidor no puede ser asignada a otro servidor si el que está actualmente asignado (servidor fuente) está encendido.
- Una ranura PCIe que tiene un adaptador asignado a un servidor no puede ser asignada a otro servidor (de destino) que está encendido.

Considere lo siguiente antes de extraer una ranura PCIe asignada de un servidor:

- Si una ranura PCIe está vacía, se la puede desasignar de un servidor, incluso si está encendido.
- Si una ranura PCIe tiene un adaptador y éste no está encendido, se la puede desasignar del servidor aunque esté encendido. Esto ocurre cuando la ranura está vacía y el servidor asignado está encendido, y un usuario introduce un adaptador en la ranura vacía.

Para obtener más información sobre la asignación y eliminación de una ranura PCIe asignada de los servidores, consulte la *Ayuda en línea*.

NOTA: Sin una licencia, puede asignar un máximo de cuatro ranuras PCIe a un servidor de altura completa, dos en la ranura superior y dos en la ranura de extensión, o dos dispositivos PCIe a un servidor de mitad de altura.

Visualización de propiedades de ranuras PCIe mediante la interfaz web del CMC

- Para ver la información acerca de las ocho ranuras PCIe, vaya al panel izquierdo y haga clic en **Descripción general del chasis → Descripción general de PCIe**. Haga clic en el + para ver todas las propiedades para la ranura requerida.
- Para ver la información acerca de una ranura PCIe, haga clic en**Descripción general del chasis → Ranura de PCIe <número> → Propiedades Estado.**

Asignación de ranuras PCIe a los servidores mediante la interfaz web del CMC

Para asignar ranuras PCIe a los servidores:

- En el panel izquierdo, haga clic en **Descripción general del chasis → Descripción general de PCIe → Configuración → Asignación: Ranuras PCIe a ranuras de servidor**. En la página **Asignación: Ranuras**

PCIe a ranuras de servidor, vaya a la columna **Acción** ubicada en el menú desplegable **Acción**, seleccione el nombre de servidor adecuado y, a continuación, haga clic en **Aplicar**.

Tenga en cuenta lo siguiente:

- Sin una licencia, se puede asignar como máximo dos ranuras PCIe a un servidor de mitad altura. Si se instala un servidor de altura completa, puede asignar dos ranuras PCIe a la ranura del servidor superior y dos a la ranura del servidor inferior (extendido), para un total de cuatro ranuras PCIe por servidor de altura completa**.**
- Puede asignar las ranuras de servidor a cualquiera de las 8 ranuras PCIe.
- Un servidor de altura completa tiene las tarjetas intermedias superior e inferior ocupadas. De lo contrario, se detendrá durante la POST cuando la <F1> o <F2> aparezca en la página para que pulse cualquier una de las teclas.
- En el caso de los servidores de altura completa, puede asignar un máximo de dos ranuras PCIe a las tarjetas intermedias superiores y dos a las inferiores. De manera predeterminada, todas las asignaciones de PCIe a la ranura 3 del servidor se dirigirán a las tarjetas intermedias inferiores.
- El número de ranura del servidor se muestra como Slot-01, Slot-02, etc. Para un servidor de altura completa, el nombre de ranura aparecerá como Ext. de Slot-01, Ext. de Slot-02, y así sucesivamente.
- Si selecciona el nombre de host, este aparecerá en lugar del nombre de la ranura.

Para obtener más información acerca de cómo asignar dispositivos PCIe a un servidor, consulte la *ayuda en línea*.

Administración de ranuras PCIe mediante RACADM

Es posible asignar o desasignar una ranura PCIe a un servidor mediante los comandos RACADM. Algunos de estos comandos están aquí provistos. Para obtener más información sobre los comandos RACADM, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia sobre líneas de comandos RACADM de Chassis Management Controller para PowerEdge VRTX) disponible en dell.com/support/Manuals.

- Para ver la asignación actual de dispositivos PCIe a servidores, ejecute el siguiente comando:
  `racadm getpiecfg -a`
- Para ver las propiedades de los dispositivos PCIe mediante FQDD, ejecute el siguiente comando:
  `racadm getpciecfg [-c <FQDD>]`

  Por ejemplo, para ver las propiedades del dispositivo PCIe 1, ejecute el siguiente comando:
  `racadm getpciecfg -c PCIE.ChassisSlot.1`
- Para asignar una ranura de adaptador PCIe a una ranura de servidor, ejecute el siguiente comando:
  `racadm setpciecfg assign [-c <FQDD>] [i <server slot>]`
- Por ejemplo, para asignar la ranura PCIe 5 a la ranura de servidor 2, ejecute el siguiente comando:
  `racadm setpciecfg assign -c PCIE.ChassisSlot.5 -i 2`
- Para desasignar una ranura PCIe 3 de un servidor, ejecute el siguiente comando:
  `racadm setpciecfg unassign -c pcie.chassisslot.3`

Protección de la alimentación de PCIe

Las tarjetas PCIe recién asignadas al CMC VRTX deben descubrirse e inicializarse antes de que se encienda el nodo de un servidor. El proceso de descubrimiento e inicialización incluye lo siguiente:

- Realizar inventario y descubrimiento de las tarjetas instaladas
- Preparar una tarjeta PCIe para la exposición a un módulo de servidor
- Preparar varias tarjetas para la configuración por parte del BIOS del servidor
- Inicialización de todas las tarjetas antes de que se encienda el nodo de un servidor blade

Todos estos procesos tardan algunos segundos en completarse, lo que ocasiona un retraso en la inicialización de las tarjetas PCIe. La función de protección de PCIe en CMC VRTX reduce el tiempo del ciclo de este proceso. La función de protección de PCIe permite lo siguiente:

- Los nodos del servidor se encienden rápidamente y, en consecuencia, también lo hacen las tarjetas PCIe.
- El estado encendido de las tarjetas PCIe se extiende durante un período de tiempo predefinido en los siguientes escenarios:
  - Una vez apagado el servidor asociado.
  - Después de que se complete el proceso de detección del adaptador.

  NOTA: Al finalizar el período de tiempo, las tarjetas PCIe se apagan. Todos los adaptadores en el modo de protección también se apagan cuando se abre la puerta del chasis.
- El estado de encendido de las tarjetas se extiende durante un tiempo predefinido después del proceso de descubrimiento. Esta extensión elimina las demoras para tipos comunes de ciclos de encendido. Las tarjetas siguen estado listas y en espera de la asignación de nodo y del encendido. Las tarjetas se apagan una vez finalizado el período de tiempo.

.

NOTA: Si el CMC no tiene suficiente alimentación, el CMC apaga todos los adaptadores en el modo de protección, con lo cual se libera toda la alimentación asignada a esos adaptadores. Si la fuente de alimentación se restablece, el consumo de energía se reasigna a las ranuras PCIe. Este tipo de restauración de la alimentación restauración permite que las tarjetas estén listas para la asignación de servidores sin demora.

Visualización de propiedades de protección de PCIe mediante la interfaz web del CMC

Para ver las propiedades de protección de PCIe, en el panel izquierdo, haga clic en **Descripción general del chasis → Descripción general de PCIe**. Aparece la página **Estado de PCIe**. La sección **Configuración general** muestra los siguientes estados de la protección de PCIe:

- **Estado de la protección**: activado o desactivado.
- **Tiempo de espera de la protección**: indica el tiempo durante el cual se activa la función de protección

Visualización del estado de las propiedades de protección de PCIe mediante RACADM

Para ver la información acerca de las propiedades de protección de la alimentación de PCIe, introduzca el siguiente comando:

```
racadm getpciecfg -r
```

Para obtener más información, consulte *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

Configuración de las propiedades de protección de PCIe mediante la interfaz web del CMC

Para configurar las propiedades de protección de PCIe para CMC VRTX:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Configuración → Protección**.

   Aparece la página **Configuración de la protección de PCIe**.
2. Para activar o desactivar la función de protección de PCIe, seleccione o borre la opción **Activar protección de PCIe** .

   NOTA: De manera predeterminada, la función de protección está activada y el período de tiempo se establece en 300 segundos.
3. En el campo **Tiempo de espera**, escriba el tiempo durante el cual la función de protección estará activada.

   Escriba cero (0) o un valor comprendido entre 60-1800 segundos. El cero indica un tiempo de espera infinito.
4. Haga clic en **Apply (Aplicar)**.

Configuración del estado de las propiedades de protección de PCIe mediante RACADM

Puede configurar las propiedades de protección de la alimentación de PCIe mediante la ejecución de los siguientes comandos:

- Para desactivar la función de protección, ejecute el comando `racadm setpciecfg ridethru -d`
- Para activar la función de protección, ejecute el comando `racadm setpciecfg ridethru -e`
- Para restablecer la propiedad de tiempo de espera de la protección, ejecute el comando `racadm setpciecfg ridethru -t <timeout>`
- Para establecer el rango de tiempo de espera aceptable, ejecute el comando `racadm setpciecfg help ridethru`

Para obtener más información, consulte la *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide (Guía de referencia de la línea de comandos RACADM de Chassis Management Controller para PowerEdge VRTX)*.

17

Solución de problemas y recuperación

En esta sección se explica cómo realizar tareas relacionadas con la recuperación y la solución de problemas en el sistema remoto a través de la interfaz web del CMC.

- Visualización de la información del chasis.
- Visualización de los registros de sucesos.
- Recopilación de información de configuración, estados de errores y registros de errores.
- Uso de la consola de diagnósticos.
- Administración de la alimentación en un sistema remoto.
- Administración de trabajos de Lifecycle Controller en un sistema remoto.
- Restablecimiento de componentes.
- Solución de problemas de protocolo de hora de red (NTP).
- Solución de problemas de red.
- Solución de problemas de alertas.
- Restablecimiento de la contraseña olvidada del administrador.
- Forma de guardar y restablecer los valores de configuración y certificados del chasis.
- Visualización de códigos y registros de errores.

Recopilación de información de configuración, estado del chasis y registros mediante RACDUMP

El subcomando `racdump` permite utilizar un solo comando para obtener información completa sobre el estado del chasis, datos de estado de configuración y registros históricos de sucesos.

El subcomando `racdump` muestra la siguiente información:

- Información general del sistema/RAC
- Información del CMC
- Información del chasis
- Información de la sesión
- Información del sensor
- Información de la compilación de firmware

Interfaces admitidas

- RACADM mediante CLI
- RACADM remoto
- RACADM mediante Telnet

`racdump` incluye los siguientes subsistemas y agrega los siguientes comandos de RACADM. Para obtener más información sobre `racdump`, consulte *RACADM Command Line Reference Guide for CMC in*

PowerEdge VRTX (Guía de referencia de la línea de comandos de RACADM para CMC en PowerEdge VRTX).

Subsistema	Comando de RACADM
Información general del sistema/RAC	`getsysinfo`
Información de la sesión	`getssninfo`
Información del sensor	`getsensorinfo`
Información de los conmutadores (módulo de E/S)	`getioinfo`
Información de la tarjeta mezzanine (tarjeta subordinada)	`getdcinfo`
Información de todos los módulos	`getmodinfo`
Información del presupuesto de alimentación	`getpbinfo`
Información de KVM	`getkvminfo`
Información del NIC (módulo CMC)	`getniccfg`
Información de redundancia	`getredundancymode`
Información del registro de rastreo	`gettracelog`
Registro de sucesos de RAC	`getraclog`
Registro de sucesos del sistema	`getsel`

Descarga del archivo MIB (Base de información de administración) SNMP

El archivo MIB SNMP del CMC define los indicadores, sucesos y tipos de chasis. El CMC permite descargar el archivo MIB a través de la interfaz web.

Para descargar el archivo Base de información de administración (MIB) SNMP del CMC a través de la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Red → Servicios → SNMP**.
2. En la sección **Configuración de SNMP**, haga clic en **Guardar** para descargar el archivo **MIB** del CMC en el sistema local.

   Para obtener más información sobre el archivo **MIB** SNMP, consulte la *Guía de referencia de SNMP de Dell OpenManage Server Administrator* disponible en **dell.com/support/manuals**.

Primeros pasos para solucionar problemas de un sistema remoto

Las preguntas siguientes se suelen utilizar para solucionar problemas de alto nivel en el sistema administrado:

- ¿El sistema se enciende o se apaga?
- Si está encendido, ¿el sistema funciona, no responde o dejó de funcionar?

- Si está apagado, ¿se ha apagado de forma imprevista?

Solución de problemas de alimentación

La información siguiente le ayudará a solucionar problemas de suministro de energía y problemas relacionados con la alimentación:

- **Problema**: se ha configurado **Política de redundancia de alimentación** en la opción **Redundancia de la red eléctrica** y se ha producido un suceso de Redundancia de suministro de energía perdida.
  - **Solución A**: esta configuración requiere al menos un suministro de energía en el lado 1 (las dos ranuras de la izquierda) y un suministro de energía en el lado 2 (las dos ranuras de la derecha) que estén presentes y en estado funcional en el gabinete modular. Además, la capacidad de cada lado debe ser suficiente para admitir el total de asignaciones de energía necesarias para que el chasis mantenga la **redundancia de cuadrícula**. (Para garantizar una operación completa de la redundancia de cuadrícula, asegúrese de que haya una configuración completa de cuatro unidades de suministro de energía).
  - **Solución B:** revise si todos los suministros de energía están correctamente conectados a las dos redes de CA. Los suministros del lado 1 deben estar conectados a una red de CA y los del lado 2 deben estar conectados a la otra red, y ambas redes de CA deben estar en funcionamiento. La **redundancia de cuadrícula** se pierde cuando una de las redes no funciona.
- **Problema:** el estado de la unidad de suministro de energía se muestra como **Error (Sin CA),** aun cuando hay conectado un cable de CA y la unidad de distribución de alimentación produce buena salida de CA.
  - **Solución A:** revise y reemplace el cable de CA. Revise y confirme que la unidad de distribución de energía que proporciona la alimentación al suministro de energía funciona como se espera. Si no se soluciona el error, comuníquese con el departamento de atención cliente de Dell para reemplazar el suministro de energía.
  - **Solución B:** revise que la unidad de suministro de energía esté conectada al mismo voltaje que las otras unidades. Si el CMC detecta que una unidad de suministro de energía está funcionando con un voltaje distinto, la unidad se apaga y se marca como fallida.
- **Problema:** la conexión dinámica del suministro de energía está activada, pero ninguno de los suministros de energía se muestra en el modo **En espera**.
  - **Resolución A:** no hay suficiente alimentación excedente. Uno o más suministros de energía pasarán al estado En espera solo cuando el excedente de alimentación disponible en el gabinete supere la capacidad de al menos un suministro de energía.
  - **Solución B:** la conexión dinámica del suministro de energía no se puede admitir por completo con las unidades de suministro de energía presentes en este gabinete. Para verificar si es así, utilice la interfaz web a fin de desactivar la conexión dinámica del suministro de energía y luego volver a activarla. Si la conexión del suministro de energía dinámica no es totalmente compatible, aparecerá un mensaje.
- **Problema:** se insertó un nuevo servidor en el gabinete con suficientes suministros de energía, pero el servidor no se enciende.
  - **Solución A:** revise la configuración del límite de alimentación de entrada del sistema; es posible que la configuración sea demasiado baja para permitir que se enciendan los servidores adicionales.
  - **Solución B:** compruebe la configuración de conservación máxima de alimentación. Este problema ocurrirá si está configurada. Para ver más detalles, consulte los valores de configuración de alimentación.
  - **Solución C:** compruebe la prioridad de alimentación de la ranura asociada con el servidor recién insertado y asegúrese de que no esté por debajo de cualquier otra prioridad de alimentación de ranura del servidor.
- **Problema:** la alimentación disponible cambia continuamente, aun cuando no haya cambiado la configuración de gabinete modular.

  - **Solución:** el CMC cuenta con administración dinámica de alimentación de ventiladores que reduce brevemente la asignación de alimentación a los servidores si el gabinete está funcionando cerca del límite máximo de alimentación configurado por el usuario; esto hace que se asigne alimentación a los ventiladores mediante la reducción del rendimiento del servidor para mantener el consumo de alimentación de entrada por debajo del **Límite de alimentación de entrada del sistema**. Se trata de un comportamiento normal.

- **Problema:** se registraron <número> vatios como **Excedente para rendimiento pico.**
  - **Solución:** el gabinete tiene <número> vatios de alimentación excedente disponible en la configuración actual y el **Límite de alimentación de entrada del sistema** puede ser reducido de forma segura a esta cantidad sin afectar el rendimiento del servidor.
- **Problema:** un subconjunto de servidores perdió alimentación después de una falla en la red de CA, aun cuando el chasis estaba operando en la configuración de **Redundancia de cuadrícula** con cuatro suministros de energía.
  - **Solución:** esto puede ocurrir si los suministros de energía se conectan incorrectamente a las redes de CA redundantes en el momento en que ocurre la falla en la red de CA. La política de **Redundancia de cuadrícula** requiere que se conecten los dos suministros de energía de la izquierda a una red de CA, y los dos suministros de energía de la derecha a otra red de CA. Si se conectan en forma inadecuada dos unidades de suministro de energía, por ejemplo, PSU2 y PSU3, a las redes de CA equivocadas, una falla en la red de CA ocasionará la pérdida de alimentación en los servidores de menor prioridad.
- **Problema:** los servidores de menor prioridad perdieron alimentación después de una falla en una unidad de suministro de energía.
  - **Solución:** para evitar que una falla futura en el suministro de energía ocasione que se apaguen los servidores, asegúrese de que el chasis tenga como mínimo tres suministros de energía y se configure de manera que la política de **Redundancia de suministro de energía** impida que la falla de una unidad de suministro de energía afecte la operación del servidor.
- **Problema:** el rendimiento general del servidor disminuye cuando aumenta la temperatura ambiente en el centro de datos.
  - **Solución:** esto puede ocurrir si el **Límite de alimentación de entrada del sistema** se configuró con un valor que provoca que una necesidad de alimentación mayor de los ventiladores se tenga que compensar con una reducción de alimentación para los servidores. El usuario puede aumentar el **Límite de alimentación de entrada del sistema** a un valor mayor de modo que se permita la asignación de alimentación adicional a los ventiladores sin afectar el rendimiento del servidor.

Solución de problemas de alertas

Use el registro del CMC y el registro de rastreo para solucionar problemas con las alertas del CMC. El éxito o la falla de cada intento de entrega de las capturas de SNMP o de correo electrónico se anota en el registro del CMC. En el registro de rastreo se incluye información adicional que describe el error específico. Sin embargo, dado que SNMP no confirma la entrega de capturas, utilice un analizador de red o una herramienta como snmputil de Microsoft para rastrear los paquetes en el sistema administrado.

Visualización de los registros de sucesos

Es posible ver los registros de hardware y del chasis para obtener información sobre los sucesos críticos del sistema que se producen en el sistema administrado.

Visualización del registro de hardware

El CMC genera un registro de sucesos de hardware que ocurren en el chasis. Para ver el registro de hardware, utilice la interfaz web y RACADM remoto.

NOTA: Para borrar el registro de hardware, debe tener privilegios de **Administrador de borrado de registros**.

NOTA: Puede configurar el CMC para enviar capturas SNMP o un correo electrónico cuando ocurran sucesos específicos. Para obtener información sobre la configuración del CMC para enviar alertas, consulte Configuración del CMC para enviar alertas.

Ejemplos de anotaciones en el registro de hardware

```
suceso crítico en el software del sistema: redundancia perdida el miércoles 09
de mayo de 2007 a las 15:26:28; suceso normal en el software del sistema:
registro guardado declarado el miércoles 09 de mayo de 2007 a las 16:06:00;
suceso de advertencia en el software del sistema: falla predictiva declarada el
miércoles 09 de mayo de 2007 a las 15:26:31; suceso crítico en el software del
sistema: registro total declarado el miércoles 09 de mayo de 2007 a las
15:47:23; suceso desconocido en el software del sistema: suceso desconocido
```

Visualización de los registros de hardware mediante la interfaz web del CMC

Es posible ver, guardar y eliminar el registro de hardware. También es posible ordenar las entradas del registro según la gravedad, fecha y hora o la descripción al hacer clic en el encabezado de la columna. Los clics posteriores que realice en los encabezados de la columna revertirán este orden.

Para ver los registros de hardware con la interfaz web del CMC, vaya al panel izquierdo y haga clic en **Descripción general del chasis** → **Registros**. Aparece la página **Registro de hardware**. Para guardar una copia del registro de hardware en la estación o red administradas, haga clic en **Guardar registro** y, a continuación, especifique una ubicación para un archivo de texto del registro.

NOTA: Dado que el registro se guarda como archivo de texto, no se mostrarán las imágenes gráficas usadas para indicar la gravedad en la interfaz de usuario. En el archivo de texto, la gravedad se indica con las palabras **Aceptar**, **Informativo**, **Desconocido**, **Advertencia** y **Grave**. Las entradas de fecha y hora aparecen en orden ascendente. Si <SYSTEM BOOT> aparece en la columna **Fecha/hora**, significa que el suceso se produjo durante el encendido o apagado de cualquiera de los módulos, cuando no hay disponible ninguna fecha ni hora.

Para borrar el registro de hardware, haga clic en **Borrar registro**.

NOTA: El CMC crea una nueva anotación de registro para indicar que el registro se borró.

NOTA: Para borrar el registro de hardware, debe tener privilegios de **Administrador de borrado de registros**.

Visualización de los registros de hardware mediante RACADM

Para ver el registro de hardware mediante RACADM, abra una consola de texto serie/Telnet/SSH en el CMC, inicie sesión y escriba:

```
racadm getsel
```

Para borrar el registro de hardware, escriba:

```
racadm clrsel
```

Visualización del registro del chasis

El CMC genera un registro de los sucesos relacionados con el chasis.

NOTA: Para borrar el registro del chasis, debe tener privilegios de **Administrador de borrado de registros**.

Visualización de los registros del chasis mediante RACADM

Para ver la información del registro del chasis mediante RACADM, abra una consola de texto serie/ Telnet/SSH en el CMC, inicie sesión y escriba lo siguiente:

```
racadm chassislog view
```

Este comando muestra las últimas 25 entradas del registro del chasis.

Para ver las opciones de visualización de chassislogs disponibles, ejecute el siguiente comando:

```
racadm chassislog help view
```

Visualización de los registros del chasis mediante la interfaz web

Puede ver, guardar y borrar el registro del chasis. Puede filtrar los registros en función del tipo de registro y filtro. Además, puede incluso realizar una búsqueda en función de una palabra clave o ver los registros en los días especificados.

En el panel izquierdo, haga clic en **Descripción general del chasis** → **Registros** → **Registro del chasis**. Se muestra la página **Registro del chasis**.

Para guardar una copia del registro del chasis en la red o Managed Station, haga clic en **Guardar registro** y luego especifique una ubicación donde guardar el archivo del registro.

Uso de la consola de diagnósticos

Puede diagnosticar los problemas relacionados con el hardware del chasis mediante los comandos de CLI si es un usuario avanzado o un usuario bajo la dirección de asistencia técnica.

NOTA: Para modificar esta configuración, debe tener privilegios de **Administrador de comandos de depuración**.

Para acceder a la consola de diagnósticos:

1. En el panel izquierdo, haga clic en **Descripción general del chasis** → **Solución de problemas** → **Diagnósticos**.

   Aparecerá la página **Consola de diagnósticos**.
2. En el cuadro de texto **Comando**, escriba un comando y haga clic en **Enviar**.

   Para obtener información acerca de los comandos, consulte la *ayuda en línea*.

   Aparece la página de resultados del diagnóstico.

Restablecimiento de componentes

Es posible restablecer el CMC activo o volver a colocar virtualmente los servidores de modo tal que se comporten como si se los hubiese quitado y vuelto a insertar. Si el chasis tiene un CMC en espera, el

restablecimiento del CMC activo produce una protección contra fallas y el CMC en espera se vuelve activo.

NOTA: Para restablecer componentes, debe tener privilegios de **Administrador de comandos de depuración**.

Para restablecer los componentes mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Solución de problemas → Restablecer componentes**.

   Aparecerá la página **Restablecer componentes**.
2. Para restablecer el CMC activo, en la sección **Estado del CMC**, haga clic en **Restablecer/Proteger contra fallas al CMC**. Si está presente un CMC en espera y un chasis es totalmente redundante, se produce una protección contra fallas, lo que provoca que el CMC en espera se vuelva activo. Sin embargo, si no hay ningún CMC en espera presente, el CMC disponible se reinicia.
3. Para volver a colocar de forma virtual el servidor, en la sección **Recolocación virtual de servidores**, seleccione los servidores que recolocará y haga clic en **Aplicar selecciones**.

   Para obtener más información, consulte la *ayuda en línea*.

   Esta operación hace que los servidores se comporten como si se hubiesen quitado e insertado nuevamente.

Guardar o restaurar la configuración del chasis

Esta es una función con licencia. Para guardar o restaurar una copia de seguridad de la configuración del chasis mediante la interfaz web del CMC:

1. En el panel izquierdo, haga clic en **Descripción del chasis → Configuración → Copia de seguridad del chasis**. Se muestra la página **Copia de seguridad del chasis**. Para guardar la configuración del chasis, haga clic en **Guardar**. Ignore la ruta de acceso del archivo (opcional) y haga clic en **Aceptar** para guardar el archivo. El archivo de copia de seguridad predeterminado contiene la etiqueta de servicio del chasis. Este archivo de copia de seguridad se puede usar posteriormente para restaurar la configuración y los certificados para este chasis solamente.
2. Para restaurar la configuración del chasis, en la sección "Restaurar", haga clic en **Examinar**, especifique el archivo de copia de seguridad y, a continuación, haga clic en **Restaurar**.

   NOTA:
   - CMC no se reinicia al restaurar la configuración; sin embargo, es posible que se requiera algo de tiempo para que los servicios del CMC asimilen los cambios o la nueva configuración. Una vez que el proceso se complete correctamente, se cerrarán todas las sesiones actuales.
   - La información de Flexaddress, los perfiles de servidores y el almacenamiento extendido no se guardan ni se restauran con la configuración del chasis.

Solución de errores de protocolo de hora de red (NTP)

Después de configurar el CMC de modo que el reloj esté sincronizado con un servidor de hora remota en la red, pueden transcurrir de 2 a 3 minutos hasta que se refleje un cambio en la fecha y hora. Si transcurrido este tiempo no se produce ningún cambio, es posible que sea necesario solucionar algún problema. El CMC no puede sincronizar el reloj por alguna de las siguientes razones:

- Es posible que haya un problema con los valores de Servidor NTP 1, Servidor NTP 2 y Servidor NTP 3.

- Es posible que se haya introducido accidentalmente un nombre de host o una dirección IP no válidos.
- Es posible que haya un problema de conectividad de red que impida que el CMC se comunique con alguno de los servidores NTP configurados.
- Podría existir un problema de DNS que impida que se resuelvan algunos nombres de host del servidor NTP.

Para solucionar estos problemas, revise la información del registro de rastreo del CMC. Este registro contiene un mensaje de error para las fallas relacionadas con NTP. Si el CMC no puede sincronizarse con los servidores NTP remotos configurados, la hora del CMC se sincronizará con el reloj del sistema local y el registro de rastreo incluirá una entrada similar a la siguiente:

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

También se puede verificar el estado de ntpd escribiendo el siguiente comando de racadm:

```
racadm getractime –n
```

La salida de este comando contiene estadísticas de NTP detalladas que pueden ser útiles para depurar el problema.

Si intenta configurar un servidor NTP basado en Windows, puede ser de utilidad aumentar el parámetro `MaxDist` de `ntpd`. Antes de cambiar este parámetro, entienda todas sus consecuencias, ya que el valor predeterminado debe ser lo suficientemente alto para que funcione con la mayoría de los servidores NTP.

Para modificar el parámetro, escriba el comando siguiente:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

Después de realizar el cambio, desactive el NTP, espere entre 5 y 10 segundos y active el NTP nuevamente:

NOTA: NTP puede tardar 3 minutos más para sincronizarse nuevamente.

Para desactivar el NTP, escriba:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

Para activar el NTP, escriba:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

Si los servidores NTP se configuraron correctamente y esta anotación está presente en el registro de rastreo, se confirmará que el CMC no puede sincronizarse con ninguno de los servidores NTP configurados.

Si no está configurada la dirección IP del servidor NTP, posiblemente verá una anotación del registro de rastreo similar a:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address
1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Si se configuró un valor del servidor NTP con un nombre de host no válido, posiblemente verá una anotación del registro de rastreo similar a:

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21
14:34:27 cmc ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

Para obtener información acerca de cómo se introduce el comando `gettracelog` a fin de revisar el registro de rastreo mediante la interfaz web del CMC, consulte Using Diagnostic Console (Uso de la consola de diagnósticos).

Interpretación de los colores y los patrones de parpadeo de los LED

Los LED en el chasis proporcionan el siguiente estado de un componente:

- Los LED que se mantienen encendidos en color verde indican que el componente está encendido. Si el LED verde está parpadeando, indica un suceso crítico pero de rutina, por ejemplo una carga de firmware, durante el cual la unidad no es operativa. Este estado no indica una falla.
- Los LED que parpadean en color ámbar en un módulo indican una falla en ese módulo.
- Los LED que parpadean en color azul pueden ser configurados por el usuario y utilizados para la identificación. Para obtener más información acerca de la configuración, consulte Configuración de los LED para identificar componentes en el chasis.

Tabla 32. Colores y patrones de parpadeo de los LED

Componente	Color de LED, patrón de parpadeo	Estado
CMC	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Activo
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Modo de espera
Servidor	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas
M. E/S (común)	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	Se está cargando el firmware
	Verde, apagado	Apagado

Componente	Color de LED, patrón de parpadeo	Estado
	Azul, encendido permanentemente	Normal/maestro de apilamiento
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas/esclavo de apilamiento
M. E/S (de paso)	Verde, encendido permanentemente	Encendido
	Verde, parpadeante	No se utiliza
	Verde, apagado	Apagado
	Azul, encendido permanentemente	Normal
	Azul, parpadeante	Identificador de módulo activado por el usuario
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Azul, apagado	Sin fallas
Ventilación	Verde, encendido permanentemente	Ventilador funcionando
	Verde, parpadeante	No se utiliza
	Verde, apagado	Apagado
	Ámbar, encendido permanentemente	Tipo de ventilador no reconocido, actualizar el firmware del CMC
	Ámbar, parpadeante	Falla del ventilador; tacómetro fuera de rango
	Ámbar, apagado	No se utiliza
PSU	(Ovalado) Verde, encendido permanentemente	CA en buen estado
	(Ovalado) Verde, parpadeante	No se utiliza
	(Ovalado) Verde, apagado	CA en mal estado
	Ámbar, encendido permanentemente	No se utiliza
	Ámbar, parpadeante	Falla
	Ámbar, apagado	Sin fallas
	(Circular) Verde, encendido permanentemente	CC en buen estado
	(Circular) Verde, apagado	CC en mal estado

Solución de problemas de un CMC que no responde

Si no puede iniciar sesión en el CMC por medio de ninguna de las interfaces (interfaz web, Telnet, SSH, RACADM remoto o serie), puede verificar la funcionalidad del CMC mediante la observación de sus indicadores LED en CMC, la obtención de información de recuperación con el puerto serie DB-9 o la recuperación de la imagen del firmware del CMC.

NOTA: No es posible iniciar sesión en el CMC en espera por medio de una consola serie.

Observación de los LED para aislar el problema

Hay dos indicadores LED en el lado izquierdo de la tarjeta:

- LED superior izquierdo: indica el estado de alimentación. Si no está ENCENDIDO:
  - Verifique que haya corriente alterna presente en al menos un suministro de energía.
  - Verifique que la tarjeta del CMC esté colocada correctamente. Puede liberar o tirar de la palanca de expulsión, extraer el CMC y volver a instalarlo asegurándose de que la placa esté insertada completamente y el seguro cierre correctamente.
- LED inferior izquierdo: este LED es de varios colores. Cuando el CMC está activo y en funcionamiento, y no hay ningún problema, el LED inferior es azul. Si es de color ámbar, se ha detectado una falla. La falla podría producirse por cualquiera de los siguientes tres sucesos:
  - Una falla del núcleo. En este caso, se debe reemplazar la placa del CMC.
  - Una falla de autoprueba. En este caso, se debe reemplazar la placa del CMC.
  - Una imagen dañada. En este caso, cargue la imagen de firmware del CMC para recuperar el CMC.

    NOTA: Un inicio o restablecimiento normal del CMC demora un poco más de un minuto para iniciar su sistema operativo completamente y quedar disponible para el inicio de sesión. El indicador LED azul está activado en el CMC activo. En una configuración redundante con dos CMC, solo el LED verde superior derecho está activado en el CMC en espera.

Obtención de la información de recuperación desde el puerto serie DB-9

Si el LED inferior es de color ámbar, la información de recuperación está disponible en el puerto serie DB-9, que se ubica en el frente del CMC.

Para obtener la información de recuperación:

1. Instale un cable de módem NULO entre el sistema CMC y el sistema cliente.
2. Abra el emulador de terminal que elija (como HyperTerminal o Minicom). Configure las siguientes especificaciones: 8 bits, sin paridad, sin control de flujo, velocidad en baudios 115200.
3. Presione la tecla <Enter>.

   Si aparece una petición de recuperación, habrá disponible información adicional. La petición indica el número de ranura del CMC y el tipo de falla.

   Para ver el motivo de la falla y la sintaxis para algunos comandos, escriba `recover` (recuperar) y presione <Enter>.

Peticiones de ejemplo:

```
recover1[self test] CMC 1 self test failure

recover2[Bad FW images] CMC2 has corrupted images
```

- Si la petición indica una falla de autoprueba, no habrá componentes utilizables en el CMC. El CMC está dañado y se debe regresar a Dell.
- Si la petición indica **Imagen del firmware dañada**, complete las tareas en la Recuperación de imagen del firmware.

Recuperación de la imagen del firmware

El CMC entra en el modo de recuperación cuando no es posible realizar un inicio normal del sistema operativo del CMC. En el modo de recuperación, hay un pequeño subconjunto de comandos disponible que permite reprogramar los dispositivos flash mediante la carga del archivo de actualización del firmware, **vrtx_cmc.bin**. Este es el mismo archivo de imagen del firmware que se utiliza para las actualizaciones normales del firmware. El proceso de recuperación mostrará su actividad actual e se inicia en el sistema operativo del CMC una vez que se completa.

Cuando escribe recover y luego presiona <Intro> en la petición recuperación, aparece el motivo de la recuperación y los subcomandos disponibles. Un ejemplo de secuencia de recuperación podría ser:

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
recover ping 192.168.0.100 recover fwupdate –g –a 192.168.0.100
```

NOTA: Conecte el cable de red al conector RJ45 del extremo izquierdo.

NOTA: En el modo de recuperación, no puede enviar comandos ping al CMC normalmente porque no hay ningún apilamiento de red activo. El comando `recover ping <TFTP server IP>` le permite enviar comandos ping al servidor TFTP para verificar la conexión de LAN. Es posible que necesite utilizar el comando `recover reset` después de `setniccfg` en algunos sistemas.

Solución de problemas de red

El registro de rastreo interno del CMC permite depurar las alertas y la red del CMC. Es posible obtener acceso al registro de rastreo a través de la interfaz web del CMC o de RACADM. Consulte la sección del comando `gettracelog` en *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guía de referencia de la línea de comandos de Chassis Management Controller para PowerEdge VRTX RACADMC).

El registro de rastreo da seguimiento a la siguiente información:

- DHCP: rastrea los paquetes que se envían a un servidor DHCP y que se reciben de él.
- DDNS: rastrea solicitudes y respuestas de actualización de DNS dinámico.
- Cambios de configuración en las interfaces de red.

El registro de rastreo también puede contener códigos de error específicos del firmware del CMC que están relacionados con el firmware interno del CMC, no con el sistema operativo del sistema administrado.

Solución de problemas de la controladora

Para solucionar los problemas de una controladora:

1. En el panel izquierdo, haga clic en **Descripción general del chasis → Almacenamiento → Controladoras → Solución de problemas**.
2. En la página **Solución de problemas de la controladora**, vaya a la lista desplegable **Acciones** de la controladora correspondiente, seleccione cualquiera de las siguientes opciones y haga clic en **Aplicar**.
   - **Restablecer configuración**: elimina los discos virtuales y las reservas activas. Sin embargo, no se borran los datos de los discos.
   - **Exportar registro TTY**: se exporta el registro de depuración TTY de la controladora de almacenamiento al sistema local.
   - **Descartar memoria caché anclada**: elimina los datos que están almacenados en la caché de la controladora RAID.

     NOTA: Si hay una caché anclada, aparece la opción para borrarla. Si no hay una caché anclada, esta opción no se muestra.
   - **Desactivar controladora RAID**: desactiva la controladora homóloga. Esta opción está disponible en el menú desplegable solamente para PERC integrado 2 cuando no está desactivado.
   - **Activar controladora RAID**: activa la controladora homóloga. Si PERC integrado 2 ya está desactivado, la opción **Activar controladora RAID** está disponible en el menú desplegable.

     NOTA:

     En caso de que PERC esté desactivado, ninguna de las demás opciones Restablecer configuración, Exportar registro de TTY, Descartar memoria caché anclada y Desactivar controladora RAID está disponible en el menú desplegable.

18

Uso de la interfaz del panel LCD

El panel LCD del chasis puede utilizarse para realizar tareas de configuración y diagnóstico, y para obtener información de estado acerca del chasis y su contenido.

En la siguiente figura se ilustra el panel LCD. La pantalla LCD muestra los menús, los iconos, los mensajes y las imágenes.

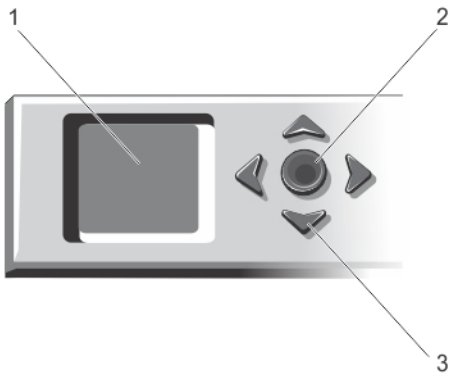


Ilustración 2. Pantalla LCD

1. Pantalla LCD
2. Botón de selección ("check")
3. Botones de desplazamiento (4)

Navegación de la pantalla LCD

El lado derecho del panel LCD tiene cinco botones: cuatro botones de flecha (arriba, abajo, izquierda y derecha) y un botón central.

- *Para desplazarse por las pantallas, use los botones de flecha derecha (siguiente) e izquierda (anterior). Mientras se usa el panel, es posible regresar a una pantalla anterior en cualquier momento.*
- *Para desplazarse a través de las opciones en una pantalla, utilice los botones de flecha hacia abajo y arriba.*
- *Para seleccionar y guardar un elemento en una pantalla y avanzar a la siguiente pantalla, utilice el botón central.*

Los botones de flecha hacia arriba, abajo, izquierda y derecha cambian los objetos o los iconos del menú seleccionados en la pantalla. El objeto seleccionado se muestra con un fondo o borde celeste.

Si la longitud de los mensajes que se muestran en la pantalla LCD excede la capacidad de la pantalla, utilice los botones de flecha hacia la izquierda y la derecha para desplazarse por el texto en esas direcciones.

Los iconos que se describen en la tabla siguiente se usan para navegar por las pantallas LCD.

Tabla 33. Iconos de navegación del panel LCD

Icono normal	Icono resaltado	Nombre y descripción del icono
		**Atrás**: seleccione y presione el botón central para regresar a la pantalla anterior.
		**Aceptar/Sí**: seleccione y presione el botón central para aceptar un cambio y regresar a la pantalla anterior.
		**Omitir/Siguiente**: seleccione y presione el botón central para omitir los cambios y avanzar a la siguiente pantalla.
		**No**: seleccione y presione el botón central para responder "No" a una pregunta y avanzar a la siguiente pantalla.
		**Identificación del componente**: parpadea el LED azul en un componente. **NOTA:** Se muestra un rectángulo azul parpadeante cerca de este icono cuando se activa la opción Identificación del componente.

El LED indicador de estado en el panel LCD indica la condición general del chasis y de sus componentes.

- Azul continuo indica que está en buenas condiciones.
- Parpadeo en color ámbar indica que al menos un componente tiene una condición de falla.
- Parpadeo en color azul es una señal de identificación que se utiliza para identificar un chasis en un grupo de chasis.

Menú principal

Desde **Menú principal**, es posible navegar a una de las siguientes pantallas:

- **Asignación de KVM (Keyboard, video and mouse)**: contiene las opciones para asignar o desasignar KVM a los servidores.
- **Asignación de DVD**: esta opción aparece en la pantalla del **Menú principal** únicamente si hay una unidad de DVD instalada.
- **Gabinete**: muestra la información de estado del chasis.
- **Resumen de IP**: muestra información sobre CMC IPv4, CMC IPv6, iDRAC IPv4 e iDRAC 4 IPv6.

- **Configuración**: contiene opciones como **Idioma del LCD**, **Orientación del chasis**, **Pantalla LCD predeterminada** y **Configuración de la red**.

Menú de asignación de KVM

En esta pantalla, puede ver el KVM de la información de asignación de servidores, asignar otro servidor al KVM o desasignar la conexión existente. Para usar el KVM para un servidor, seleccione **Asignación de KVM** en el menú principal, navegue hasta el servidor correspondiente y, a continuación, presione el botón central **Check** (Verificar).

Asignación de DVD

Al utilizar esta página, es posible ver la información sobre la asignación de DVD a un servidor, asigne otro servidor a la unidad de DVD en el chasis, o bien, anule la asignación de la conexión existente. Para que el servidor tenga acceso a la unidad de DVD, seleccione **Asignación de DVD** en el menú principal, navegue hasta el servidor requerido y, a continuación, presione el botón central **Check** (Verificar).

Es posible asignar la unidad de DVD a la ranura del servidor solamente si dicha unidad se encuentra activada para esa ranura del servidor. Asimismo, también se puede anular la asignación de la unidad de DVD para evitar que se utilice en las ranuras del servidor. Si el cable SATA no se conecta correctamente entre la unidad de DVD y la placa principal, la condición de la unidad de DVD será crítica. Si la condición de la unidad de DVD es crítica, el servidor no puede acceder a ella.

NOTA: La función Asignación de DVD aparece en la pantalla **Menú principal** del LCD solo si hay una unidad de DVD instalada.

Menú del alojamiento

Esta pantalla permite obtener acceso a las siguientes pantallas:

- **Estado de la parte delantera**
- **Estado de la parte posterior**
- **Estado de la parte lateral**
- **Estado del gabinete**

Use los botones de navegación para seleccionar el elemento correspondiente (seleccione el icono **Atrás** para regresar a **Menú principal**) y presione el botón central. Se mostrará la pantalla seleccionada.

Menú Resumen de IP

La pantalla **Resumen de IP** muestra la información de IP del CMC (IPv4 y IPv6) y de cada servidor que está instalado en el chasis.

Use los botones de flechas hacia arriba y hacia abajo para desplazarse por la lista. Use las flechas hacia la izquierda y hacia la derecha para desplazarse por los mensajes seleccionados que no caben en la pantalla.

Use los botones de flechas hacia arriba y hacia abajo para seleccionar el icono **Atrás** y presione el botón central para regresar al menú **Gabinete**.

Configuración

El menú **Configuración** muestra diversos elementos que pueden configurarse:

- **Idioma del LCD**: seleccione el idioma que desea utilizar para el texto y los mensajes de la pantalla LCD.
- **Orientación del chasis**: seleccione la opción **Modo torre** o bien **Modo bastidor** según la orientación del chasis durante la instalación.
- **Pantalla LCD predeterminada**: seleccione la pantalla (**Menú principal**, **Estado de la parte delantera**, **Estado de la parte posterior**, **Estado de la parte lateral** o **Personalizado**) que aparece cuando no hay actividad en el panel LCD.
- **Configuración de la red**: seleccione esta opción para configurar la red de un CMC. Para obtener más información acerca de esta función, consulte la Configuración de la red CMC mediante la interfaz del panel LCD.

Utilice los botones de flecha hacia arriba y abajo para resaltar una opción del menú o seleccione el icono **Atrás** si desea regresar al **Menú principal**.

Para activar la selección, presione el botón del centro.

Idioma de LCD

La pantalla **Idioma de LCD** permite seleccionar el idioma usado para los mensajes del panel LCD. El idioma actualmente activo está resaltado con un fondo celeste.

1. Use los botones de flecha hacia arriba, hacia abajo, hacia la izquierda y hacia la derecha para resaltar el idioma deseado.
2. Presione el botón central. Aparecerá el icono **Aceptar** resaltado.
3. Presione el botón central para confirmar el cambio. Aparecerá el menú **Configuración de LCD**.

Pantalla predeterminada

La opción **Pantalla predeterminada** permite cambiar la pantalla que el panel LCD muestra cuando no hay ninguna actividad en el panel. La pantalla predeterminada de fábrica es **Menú principal.** Puede elegir entre las siguientes pantallas:

- **Menú principal**
- **Estado frontal** (vista gráfica frontal del chasis)
- **Estado posterior** (vista gráfica posterior del chasis)
- **Estado lateral** (vista gráfica izquierda del chasis)
- **Personalizado** (logotipo de Dell con nombre del chasis)

La pantalla actualmente activa aparece resaltada en celeste.

1. Utilice los botones de flecha hacia arriba y abajo para resaltar la pantalla que desea definir como predeterminada.
2. Presione el botón central. El icono **Aceptar** aparecerá resaltado.
3. Vuelva a presionar el botón central para confirmar el cambio. Aparecerá **Pantalla predeterminada**.

Diagnóstico

El panel LCD permite diagnosticar problemas en cualquier servidor o módulo del chasis. Si hay un problema o se produjo una falla en el chasis, en cualquier servidor o en cualquier módulo del chasis, el

indicador de estado del panel LCD parpadea en color ámbar. En el **Menú principal**, un icono con fondo ámbar aparece junto al elemento del menú (Gabinete) que conduce al estado de la parte posterior, frontal, lateral o de gabinete.

Al seguir los iconos color ámbar a través del sistema de menús de la pantalla LCD, es posible visualizar la pantalla de estado y los mensajes de error del elemento que presenta el problema.

Los mensajes de error del panel LCD pueden quitarse al eliminar el módulo o el servidor que causa el problema o borrar el registro de hardware del módulo o servidor. En los errores del servidor, use la interfaz web o la interfaz de línea de comandos del iDRAC para borrar el Registro de sucesos del sistema (SEL) del servidor. En los errores del chasis, use la interfaz web o la interfaz de línea de comandos del CMC para borrar el registro de hardware.

Mensajes de la pantalla LCD del panel frontal

Esta sección incluye dos apartados que muestran los mensajes de error y la información de estado que aparecen en la pantalla LCD del panel frontal.

Los *mensajes de error* de la pantalla LCD tienen un formato similar al del registro de sucesos del sistema (SEL) que se visualiza en la interfaz web o en CLI.

La tabla en la sección de errores muestra los mensajes de error y de advertencia que aparecen en las diferentes pantallas LCD y la causa posible de cada mensaje. El texto entre comillas angulares (< >) indica que el texto puede variar.

Información de estado en la pantalla LCD incluye información descriptiva sobre los módulos del chasis. Las tablas en esta sección describen la información que se muestra para cada componente.

Información de estado del servidor y del módulo de LCD

En las tablas que figuran en esta sección se describen las opciones de estado que se muestran en la pantalla LCD del panel frontal para cada tipo de componente del chasis.

Tabla 34. Estado del CMC

Elemento	Descripción
Nombre/Ubicación	Ejemplo: CMC1, CMC2
Sin errores	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Firmware Version	Solo se muestra en un CMC activo. Muestra el mensaje “En espera” para el CMC que está en espera.
IP4 <activado, desactivado>	Muestra el estado actual activado de IPv4 únicamente en un CMC activo.
Dirección IP4: <dirección, adquiriendo>	Solo se muestra si IPv4 está activado únicamente en un CMC activo.

Elemento	Descripción
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.
MAC: <dirección>	Muestra la dirección MAC del CMC.

Tabla 35. Estado del chasis o del gabinete

Elemento	Descripción
Nombre definido por el usuario	Ejemplo: "Sistema de bastidor Dell". Esto puede configurarse con la CLI del CMC o la interfaz web.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Número de modelo	Ejemplo: "PowerEdgeM1000".
Consumo de alimentación	Consumo de alimentación actual en vatios.
Alimentación pico	Consumo de alimentación pico en vatios.
Alimentación mínima	Consumo mínimo de alimentación en vatios.
Temperatura ambiente	Temperatura ambiente actual en grados Celsius.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.
Modo de redundancia del CMC	No redundante o Redundante.
Modo de redundancia de la unidad de suministro de energía	No redundante, Redundancia de cuadrícula o Redundancia de CC.

Tabla 36. Estado del ventilador

Elemento	Descripción
Nombre/Ubicación	Ejemplo: Fan1, Fan2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
RPM	Velocidad actual del ventilador en RPM.

Tabla 37. Estado de la unidad de suministro de energía

Elemento	Descripción
Nombre/Ubicación	Ejemplo: PSU1, PSU2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más

Elemento	Descripción
	importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Status	Desconectado, conectado o en espera: indica el estado de la alimentación de una unidad de suministro de energía.
Potencia máxima	Potencia máxima que la unidad de suministro de energía puede proporcionar al sistema.

Tabla 38. Estado del módulo de E/S

Elemento	Descripción
Nombre/Ubicación	Módulo de E/S A
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Status	Apagado o encendido: indica si el M. E/S está funcionando.
Model	Modelo del módulo de E/S.
Tipo de red Fabric	Tipo de sistema de red.
Dirección IP	Solo se muestra si los módulos de E/S están encendidos. En el tipo de módulo de E/S de paso el valor es cero.
Etiqueta de servicio	Etiqueta de servicio asignada en fábrica.

Tabla 39. Estado de asignación de KVM

Elemento	Descripción
Servidor <número>	Muestra una lista de los servidores a los que se les puede asignar KVM.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Asignado	Muestra una lista de los servidores asignados a un KVM, si los hubiera.
Ranura <número>	Indica la ranura del servidor a la que el KVM está asignado. Los valores posibles son SLOT-*<01 a 04>*.
Desasignado	Se muestra si el KVM no está asignado a ninguno de los servidores.

Tabla 40. Estado de asignación de DVD

Elemento	Descripción
Servidor <número>	Muestra una lista de los servidores a los que se les puede asignar el DVD.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Asignado	Muestra una lista de los servidores asignados a un DVD, si los hubiera.
Ranura <número>	Indica la ranura del servidor a la que el DVD está asignado. Los valores posibles son SLOT- *<01 a 04>*.
Desasignado	Se muestra si el KVM no está asignado a ninguno de los servidores.

Tabla 41. Estado del ventilador

Elemento	Descripción
Nombre/Ubicación	Ejemplo: Blower1, Blower2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
RPM	Velocidad actual del ventilador en RPM.

Tabla 42. Estado de SPERC

Elemento	Descripción
SPERC: <número>	Muestra el nombre de SPERC en el formato SPERC n, donde 'n' es el número de SPERC. Ejemplo: SPERC 1, SPERC 2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Estado del trabajo	Activado o desactivado: indica si la SPERC está en funcionamiento.
Nombre: <nombre>	Nombre de Shared PERC. Ejemplo: SPERC8
Estado de condición	En buen estado
Firmware Version	Versión del SPERC
Fabricante	Nombre del fabricante

Elemento	Descripción
Status	Desconectado, conectado o en espera: indica el estado de alimentación de un SPERC.

Tabla 43. Estado de la tarjeta PCIe

Elemento	Descripción
Tarjeta PCIe <*número*>	Muestra el nombre de la tarjeta PCIe en el formato Tarjeta PCIe <*n*>, donde "n" es el número de la tarjeta PCIe. Ejemplo: Tarjeta PCIe 1, Tarjeta PCIe 2, y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Estado del trabajo	Activado o desactivado: indica si la tarjeta PCIe está en funcionamiento.
Nombre: <nombre>	Nombre de la tarjeta PCIe.
Asignada a un servidor	Asignada o desasignada.

Tabla 44. Estado de la unidad de disco duro

Elemento	Descripción
Unidad de disco duro: <número>	Muestra el nombre de la unidad de disco duro en el formato de la unidad de disco duro <*n*>, donde 'n' es el número de la unidad de disco duro. Ejemplo: Unidad de disco duro 1, unidad de disco duro 2 y así sucesivamente.
Mensajes de error	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde las más importantes son los primeros de la lista y, a continuación, los mensajes relacionados con avisos.
Estado de la alimentación	Rotación alta, transición, rotación baja: indica el estado de la alimentación de una unidad de disco duro
Fabricante	Nombre del fabricante
Capacity	La capacidad de almacenamiento disponible de la unidad de disco duro en gigabytes (GB)
Versión del firmware	Muestra la versión del firmware de la unidad de disco duro
Status	Desconectado, conectado o en espera: indica el estado de la alimentación de la unidad de disco duro.

Tabla 45. Estado del servidor

Elemento	Descripción
Nombre/Ubicación	Ejemplo: Servidor 1, Servidor 2, y así sucesivamente.
Sin errores	Si no hay errores, se mostrará el mensaje Sin errores. De lo contrario, aparecen los mensajes de error, donde los más importantes aparecen primero en la lista y, a continuación, los mensajes relacionados con avisos. Para obtener más información, consulte "Mensajes de error de la pantalla LCD".
Nombre de ranura	Nombre de ranura del chasis. Por ejemplo, RANURA-01. **NOTA:** Puede configurar esta tabla a través de la CLI o la interfaz web del CMC.
Name	Nombre del servidor, que el usuario puede establecer mediante Dell OpenManage. El nombre se muestra únicamente si el iDRAC completó el inicio y si el servidor admite esta función; en caso contrario, se muestran los mensajes de inicio de iDRAC.
Número de modelo	Se muestra si el iDRAC completó el inicio.
Etiqueta de servicio	Se muestra si el iDRAC completó el inicio.
Versión del BIOS	Versión del firmware del BIOS del servidor.
Último código de la POST	Muestra la cadena de mensajes del último código de la POST del BIOS del servidor.
Versión del firmware del iDRAC	Se muestra si el iDRAC completó el inicio. **NOTA:** La versión del iDRAC 1.01 se muestra como 1.1. No hay versión 1.10 del iDRAC.
IP4 <activado, desactivado>	Muestra el estado actual activado del IPv4.
Dirección IP4: <dirección, adquiriendo>	Solo se muestra si IPv4 está activado.
IP6 <activado, desactivado>	Solo se muestra si el iDRAC admite IPv6. Muestra el estado actual activado del IPv6.
Dirección local IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
Dirección global IP6: <dirección>	Solo se muestra si iDRAC admite IPv6 y si IPv6 está activado.
FlexAddress activado en la red Fabric	Solo se muestra si la función está instalada. Enumera las redes Fabric activadas para dicho servidor (es decir, A, B, C).

La información de la tabla se actualiza de forma dinámica. Si el servidor no admite esta función, la siguiente información no aparecerá; en caso contrario, las opciones de Server Administrator son las siguientes:

- Opción “Ninguna” = No se debe mostrar ninguna cadena en la pantalla LCD.
- Opción “Predeterminada” = Ningún efecto.
- Opción “Personalizada” = Permite introducir un nombre de cadena para el servidor.

La información se muestra únicamente si el iDRAC completó el inicio. Para obtener más información sobre esta función, consulte *RACADM Command Line Reference Guide for CMC in PowerEdge VRTX (Guía de referencia de la línea de comandos RACADM para CMC en PowerEdge VRTX)*.

19

Preguntas frecuentes

En esta sección se enumeran las preguntas frecuentes para los elementos siguientes:

- RACADM
- Administración y recuperación de un sistema remoto
- Active Directory
- FlexAddress y FlexAddressPlus
- M. E/S

RACADM

Después de restablecer el CMC (con el subcomando RACADM racreset), al introducir un comando, se muestra el siguiente mensaje:

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

¿Qué significa este mensaje?

Debe ejecutarse otro comando únicamente después de que el CMC termine de restablecerse.

Al usar subcomandos RACADM a veces se muestra uno o más de los siguientes errores:

- Mensajes de errores locales: problemas de sintaxis, errores tipográficos y nombres incorrectos. Ejemplo: `ERROR: <message>`

  Use el subcomando RACADM `help` para ver la información de uso y sintaxis correcta. Por ejemplo, si se produce un error al borrar el registro del chasis, ejecute el siguiente subcomando:

  ```
  racadm chassislog help clear
  ```
- Mensajes de error relacionados con el CMC: problemas en los que el CMC no puede ejecutar una acción. Aparece el siguiente mensaje de error:

  ```
  racadm command failed.
  ```

Para ver información sobre un chasis, escriba el siguiente comando:

```
racadm gettracelog
```

Durante el uso del RACADM del firmware, la petición cambia a ">" y la petición "$" ya no se muestra.

Si escribe un solo carácter de comillas dobles (") o simple (') sin el cierre correspondiente en el comando, la CLI cambiará a ">" y pondrá todos los comandos en cola.

Para regresar a la petición "$", presione <Ctrl>–d:

Se mostrará el mensaje de error `Not Found` al utilizar los comandos `$ logout` y `$ quit`.

Administración y recuperación de un sistema remoto

¿Por qué no están disponibles RACADM remoto y los servicios web después de un cambio de propiedad?

Es posible que los servicios de RACADM remoto y de la interfaz web tarden un minuto para estar disponibles después de que el componente Web Server del CMC se restablece.

El Web Server del CMC se restablece después de que se producen los siguientes acontecimientos:

- Se cambia la configuración de la red o las propiedades de seguridad de la red por medio de la interfaz de usuario web del CMC.
- Se cambia la propiedad cfgRacTuneHttpsPort (incluso cuando un comando config -f <archivo de configuración> la cambia).
- Se utiliza `racresetcfg` o se restablece una copia de seguridad de la configuración del chasis.
- Se restablece el CMC.
- Se carga un nuevo certificado del servidor SSL.

¿Mi servidor DNS no registra mi CMC?

Algunos servidores DNS solo registran nombres de 31 caracteres como máximo.

Al obtener acceso a la interfaz web del CMC, aparece una advertencia de seguridad que indica que el certificado SSL fue emitido por una autoridad de certificados que no es confiable.

El CMC incluye un certificado de servidor del CMC predeterminado para garantizar la seguridad de la red en las funciones de la interfaz web y de RACADM remoto. Este certificado no es emitido por una autoridad de certificados confiable. Para solucionar este problema de seguridad, cargue un certificado de servidor del CMC que haya sido emitido por una autoridad de certificados confiable (por ejemplo, Thawte o Verisign).

¿Por qué se muestra el mensaje siguiente por motivos desconocidos?

Remote Access: SNMP Authentication Failure

Como parte del descubrimiento, IT Assistant intenta verificar los nombres de comunidad **Get** y **Set** del dispositivo. En IT Assistant, usted tiene el nombre de **comunidad get = public** y el **nombre de comunidad set = private**. De manera predeterminada, el nombre de comunidad para el agente CMC es "public". Cuando IT Assistant envía una solicitud de comunidad Set, el agente CMC genera el error de autentificación SNMP porque solo acepta solicitudes de **comunidad = public**.

Cambie el nombre de comunidad del CMC desde RACADM. Para ver el nombre de comunidad del CMC, use el siguiente comando:

```
racadm getconfig -g cfgOobSnmp
```

Para establecer el nombre de comunidad del CMC, utilice el siguiente comando:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
```

Para evitar que se generen capturas de autentificación SNMP, debe utilizar nombres de comunidad que acepte el agente. Como el CMC solo permite un nombre de comunidad, debe introducir el mismo nombre de comunidad Get y Set para la configuración de descubrimiento de IT Assistant.

Al obtener acceso a la interfaz web del CMC, se muestra una advertencia de seguridad que indica que el nombre de host del certificado SSL no coincide con el nombre de host del CMC.

El CMC incluye un certificado de servidor del CMC predeterminado para garantizar la seguridad de la red en las funciones de la interfaz web y de RACADM remoto. Cuando se utiliza este certificado, el explorador web muestra una advertencia de seguridad cuando el certificado predeterminado no coincide con el nombre de host del CMC (por ejemplo, la dirección IP).

Para solucionar este problema de seguridad, cargue un certificado de servidor del CMC que haya sido emitido para la dirección IP del CMC. Al generar la solicitud de firma de certificado (CSR) que se utilizará para emitir el certificado, asegúrese de que el nombre común (CN) de la CSR tenga la misma dirección IP que el CMC (por ejemplo, 192.168.0.120) o el mismo nombre DNS registrado del CMC.

Para asegurarse de que la CSR coincida con el nombre DNS registrado del CMC:

1. En el panel izquierdo, haga clic en **Descripción general del chasis.**
2. Haga clic en **Red**.
   Aparecerá la página **Configuración de la red**.
3. Seleccione la opción **Registrar el CMC en DNS**.
4. Introduzca el nombre del CMC en el campo **Nombre del CMC de DNS**.
5. Haga clic en **Aplicar cambios**.

Active Directory

¿Admite Active Directory el inicio de sesión en el CMC en varios árboles?

Sí. El algoritmo de consulta de Active Directory del CMC admite varios árboles en un solo bosque.

¿El inicio de sesión en el CMC mediante Active Directory funciona en el modo mixto (es decir, los controladores de dominio del bosque ejecutan diferentes sistemas operativos, como Microsoft Windows 2000 o Windows Server 2003)?

Sí. En el modo mixto, todos los objetos utilizados por el proceso de consulta del CMC (entre el usuario, el objeto del dispositivo del RAC y el objeto de asociación) tienen que estar en el mismo dominio.

El complemento Usuarios y equipos de Active Directory extendido por Dell verifica el modo y limita a los usuarios a fin de crear objetos en varios dominios si se encuentra en modo mixto.

¿El uso del CMC con Active Directory admite varios entornos de dominio?

Sí. El nivel de la función del bosque de dominios debe estar en el modo Nativo o en el modo Windows 2003. Asimismo, los grupos entre el objeto de asociación, los objetos de usuario de RAC y los objetos de dispositivo de RAC (incluido el objeto de asociación) deben estar en grupos universales.

¿Estos objetos extendidos por Dell (objeto de asociación Dell, dispositivo de RAC de Dell y objeto de privilegio Dell) pueden estar en dominios diferentes?

El objeto de asociación y el objeto de privilegio deben estar en el mismo dominio. El complemento Usuarios y equipos de Active Directory extendido por Dell permite crear estos dos objetos solamente en el mismo dominio. Otros objetos pueden estar en diferentes dominios.

¿Existe alguna restricción para la configuración del controlador de dominio de SSL?

Sí. Todos los certificados SSL para los servidores Active Directory que se encuentran en el bosque deben estar firmados mediante el mismo certificado con firma de la autoridad de certificados raíz, pues el CMC solo permite cargar un certificado SSL firmado por una autoridad de certificados de confianza.

La interfaz web no se inicia una vez que se creó y se cargó un nuevo certificado RAC.

Si se utilizan los servicios de certificados de Microsoft para generar el certificado RAC, es posible que se haya utilizado la opción Certificado de usuario en lugar de Certificado web durante la creación del certificado.

Para solucionar el problema, genere una CSR, cree un certificado web nuevo mediante el uso de los servicios de certificados de Microsoft y cárguelo por medio de ejecutar los siguientes comandos de RACADM:

```
racadm sslcsrgen [-g] [-f {nombre de archivo}]

racadm sslcertupload -t 1 -f {cert_SSL_de_web}
```

FlexAddress y FlexAddressPlus

¿Qué sucede si se quita una tarjeta de función?

No se producen cambios visibles al quitar una tarjeta de función. Este tipo de tarjetas pueden quitarse y almacenarse, o bien, pueden dejarse colocadas.

¿Qué sucede si se quita una tarjeta de función que se utilizó en un chasis y se coloca en otro?

La interfaz web muestra el siguiente mensaje de error:

```
This feature card was activated with a different chassis. It must be removed
before accessing the FlexAddress feature.

Current Chassis Service Tag = XXXXXXXX

Feature Card Chassis Service Tag = YYYYYYYY

Se agrega una anotación al registro del CMC que indica:

cmc <fecha de marca de tiempo>: función "FlexAddress@YYYYYYY" no activada;
identificación del chasis = "XXXXXXX"
```

¿Qué sucede si se quita la tarjeta de función y se instala una tarjeta que no sea de FlexAddress?

No se activa ni se modifica la tarjeta. El CMC ignora la tarjeta. En este caso, el comando **$racadm featurecard -s** muestra el siguiente mensaje:

```
No feature card inserted

ERROR: can't open file (No se insertó ninguna tarjeta de función. ERROR: no se puede abrir el archivo).
```

Si se reprograma la etiqueta de servicio del chasis, ¿qué sucede si hay una tarjeta de función vinculada a ese chasis?

- Si la tarjeta de función original está presente en el CMC activo en ese u otro chasis, la interfaz web muestra el siguiente mensaje de error:

  ```
  This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.

  Current Chassis Service Tag = XXXXXXXX

  Feature Card Chassis Service Tag = YYYYYYYY
  ```

  The original feature card is no longer eligible for deactivation on that or any other chassis, unless Dell Service reprograms the original chassis service tag back into a chassis, and CMC that has the original feature card is made active on that chassis.
- La función FlexAddress continúa activada en el chasis vinculado originalmente. La vinculación de esa función del chasis se actualiza y refleja la nueva etiqueta de servicio.

¿Se muestra un mensaje de error si hay dos tarjetas de función instaladas en el sistema de CMC redundante?

La tarjeta de función del CMC activo está activa e instalada en el chasis, en tanto que la segunda tarjeta es ignorada por el CMC.

¿La tarjeta SD tiene un dispositivo de protección contra escritura?

Sí. Antes de instalar la tarjeta SD en el módulo de CMC, verifique que el seguro de protección contra escritura esté desbloqueado. La función FlexAddress no podrá activarse si la tarjeta SD está protegida contra escritura. En este caso, el comando **$racadm feature -s** muestra el siguiente mensaje:

```
No features active on the chassis. ERROR: read only file system (No hay funciones activas en el chasis. ERROR: sistema de archivo de solo lectura).
```

¿Qué sucede si no hay una tarjeta SD en el módulo CMC activo?

El comando **$racadm featurecard -s** muestra este mensaje:

```
No se insertó ninguna tarjeta de función.
```

¿Qué le sucede a la función FlexAddress si el BIOS del servidor se actualiza de la versión 1.xx a la versión 2.xx?

Se debe apagar el módulo del servidor para poder usarlo con FlexAddress. Una vez completada la actualización del BIOS del servidor, el módulo del servidor no recibirá direcciones asignadas por el chasis hasta que se haya activado el ciclo de encendido del servidor.

¿Cómo se puede recuperar una tarjeta SD si no se encontraba en el chasis al ejecutar el comando de desactivación en FlexAddress?

El problema es que la tarjeta SD no puede utilizarse para instalar FlexAddress en otro chasis si no se encontraba en el CMC al momento de desactivar FlexAddress. Para recuperar el uso de la tarjeta, insértela de nuevo en un CMC del chasis con el que esté vinculada, reinstale FlexAddress y luego desactive FlexAddress nuevamente.

La tarjeta SD está correctamente instalada y se realizaron todas las actualizaciones de firmware y software. La función FlexAddress está activa, pero la pantalla de implementación del servidor no muestra las opciones para implementarla. ¿Cuál es el problema?

Este es un problema de almacenamiento en caché del explorador. Cierre sesión en el explorador e inícielo nuevamente.

¿Qué sucede con FlexAddress si debo restablecer la configuración del chasis con el comando RACADM racresetcfg?

La función FlexAddress permanece activada y disponible. Se seleccionan en forma predeterminada todas las ranuras y redes Fabric.

NOTA: Se recomienda especialmente apagar el chasis antes de ejecutar el comando RACADM `racresetcfg`.

Después de desactivar únicamente la función FlexAddressPlus (dejando activada FlexAddress), ¿por qué falla el comando racadm setflexaddr en el CMC (aún activo)?

Si el CMC posteriormente pasa a estar activo, y la tarjeta de función FlexAddressPlus está insertada en la ranura, la función FlexAddressPlus se reactiva y es posible reanudar los cambios de la configuración de FlexAddress para ranuras y redes Fabric.

Módulos de E/S

Después de realizar un cambio en la configuración, algunas veces, el CMC muestra la dirección IP 0.0.0.0.

Haga clic en el icono **Actualizar** para ver si la dirección IP está correctamente configurada en el conmutador. Si se comete un error al configurar la dirección IP, la máscara o la puerta de enlace, el conmutador no configurará la dirección IP y mostrará 0.0.0.0 en todos los campos.

Errores comunes:

- Configurar la dirección IP fuera de banda con el mismo valor que la dirección IP de administración en banda o en la misma red que esta última.
- Introducir una máscara de subred no válida.
- Configurar la puerta de enlace predeterminada con una dirección que no está en una red directamente conectada al conmutador.