Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise para servidores blade versión 3.5

Guía del usuario

Notas y precauciones

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

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

La información contenida en esta publicación puede modificarse sin previo aviso.
© 2013 Dell Inc. Todos los derechos reservados.

Queda estrictamente prohibida la reproducción de este material en cualquier forma sin la autorización por escrito de Dell Inc.

Marcas comerciales utilizadas en este texto: Dell™, el logotipo de DELL™, OpenManage™ y PowerEdge™ son marcas comerciales de Dell Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, Windows Vista®, MS-DOS™, ActiveX™ y Active Directory® son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y/o en otros países. Red Hat® y Red Hat Enterprise Linux® son marcas comerciales registradas de Red Hat, Inc. en los Estados Unidos y en otros países. Novell® y SUSE® son marcas comerciales registradas de Novell Inc. en los Estados Unidos y en otros países. Intel® y Pentium® son marcas comerciales registradas de Intel Corporation en los Estados Unidos y en otros países. UNIX® es una marca comercial registrada de The Open Group en los Estados Unidos y en otros países. Thawte® es una marca comercial registrada de Thawte Consulting (Pty) Ltd. VeriSign® es una marca comercial registrada de VeriSign, Inc. y sus filiales en los Estados Unidos y países extranjeros. Sun™ y Java™ son marcas comerciales o marcas comerciales registradas de Oracle Corporation o sus filiales en los Estados Unidos y en otros países. Mozilla® y Firefox® son marcas comerciales registradas de Mozilla Foundation. Fedora™ es una marca comercial de Red Hat, Inc.

Copyright 1998-2009 The OpenLDAP Foundation. Todos los derechos reservados. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, solo según lo autoriza la licencia pública de OpenLDAP. Una copia de esta licencia está disponible en el archivo LICENSE en el directorio principal de la distribución, o bien, en **OpenLDAP.org/license.html**. OpenLDAP es una marca comercial registrada de OpenLDAP Foundation. Hay archivos individuales y/o paquetes recibidos en contribuciones que pueden ser propiedad intelectual de terceros y están sujetos a restricciones adicionales. Este trabajo se deriva de la distribución LDAP v3.3 de la Universidad de Michigan. Este trabajo también contiene materiales que provienen de fuentes públicas. La información acerca de OpenLDAP se puede obtener en **openldap.org/**. Porciones de Copyright 1998-2004 Kurt D. Zeilenga. Porciones de Copyright 1998-2004 Net Boolean Incorporated. Porciones de Copyright 2001-2004 IBM Corporation. Todos los derechos reservados.
Se permite la redistribución y el uso en formatos binario y original, con o sin modificaciones, sólo de la manera que lo autoriza la licencia pública de OpenLDAP. Porciones de Copyright 1999-2003 Howard Y.H. Chu. Porciones de Copyright 1999-2003 Symas Corporation. Porciones de Copyright 1998-2003 Hallvard B. Furuseth. Todos los derechos reservados. Se permite la redistribución y uso en formatos binario y original, con o sin modificaciones, siempre y cuando se conserve este aviso. Los nombres de los titulares de la propiedad intelectual no se deben usar para promocionar o promover productos derivados de este software sin previo permiso escrito específico. Este software se ofrece “tal cual” sin garantías expresas o implícitas. Porciones de Copyright (c) 1992-1996 Regentes de la Universidad de Michigan. Todos los derechos reservados. Se permite la redistribución y uso en formatos binario y original siempre y cuando se conserve este aviso y se conceda el crédito correspondiente a la Universidad de Michigan en Ann Arbor. El nombre de la universidad no se debe usar para promocionar ni promover productos derivados de este software sin previo permiso específico por escrito. Este software se ofrece “tal cual” sin garantías expresas o implícitas.

Otras marcas y otros nombres comerciales pueden utilizarse en este documento para hacer referencia a las entidades que los poseen o a sus productos. Dell Inc. renuncia a cualquier interés sobre la propiedad de marcas y nombres comerciales que no sean los suyos.

03/2013

Contenido

1 Descripción general del iDRAC6 Enterprise 21

Novedades de esta versión **22**

Certificación IPv6 Ready Logo **22**

Características de seguridad del iDRAC6 . . . . . **23**

iDRAC6 Enterprise y tarjeta multimedia vFlash **24**

Plataformas admitidas **26**

Sistemas operativos compatibles **27**

Exploradores web admitidos **27**

Conexiones de acceso remoto admitidas **27**

Puertos del iDRAC6 . . . . . **28**

Otros documentos que podrían ser útiles **29**

Acceso a los documentos desde el sitio web del servicio de asistencia Dell Support **31**

2 Configuración de iDRAC6 Enterprise . . . 33

Antes de comenzar **33**

Interfaces para configurar el iDRAC6 . . . . . **33**

Tareas de configuración **37**
Configurar la estación de administración 37
Configurar el sistema de red del iDRAC6 37
Configurar los usuarios de iDRAC6 38
Configurar servicios de directorios 38
Configurar la filtración y el bloqueo de IP 39
Configurar los sucesos de plataforma 39
Activación o desactivación del acceso a la configuración local 40
Configurar los servicios del iDRAC6 40
Configurar la capa de sockets seguros (SSL) . . . 40
Configurar los medios virtuales 41
Configurar una tarjeta multimedios vFlash 41
Instalación del software de servidor administrado 41
Configure el servidor administrado para utilizar la función de pantalla de último bloqueo 41

Configuración de la red por medio de la interfaz web del CMC **42**
Iniciar la interfaz web del iDRAC6 desde el CMC 42
Configuración de la conexión de red de iDRAC6 43

Visualización de las conexiones de red Fabric de la tarjeta mezzanine FlexAdress **44**
Dirección MAC de FlexAddress para iDRAC6 . . . 46

Registro del sistema remoto **47**

Primer dispositivo de inicio **49**

Recurso compartido de archivos remotos **50**

Módulo SD dual interno **53**

Visualización del estado del módulo de SD doble interno mediante la interfaz gráfica de usuario 54

Actualización del firmware de iDRAC6 . . . . . **55**

Descarga del firmware o el paquete de actualización 55

Ejecutar la actualización del firmware 56

Verificación de la firma digital para los DUP de Linux 57

Uso de la interfaz web del iDRAC6 60

Actualización del firmware del iDRAC6 por medio de RACADM 62

Uso de la utilidad de actualización de DOS 62

Uso de la interfaz WSMAN 63

Actualización del paquete de reparación de USC **63**

Configuración del iDRAC6 para utilizarlo con IT Assistant **63**

Uso de la utilidad de configuración del iDRAC6 para activar las funciones de descubrimiento y supervisión **64**

Uso de la interfaz web del iDRAC6 para activar las funciones de descubrimiento y supervisión **65**

Uso de IT Assistant para ver el estado y los sucesos del iDRAC6 . . . . . **67**

3 Configuración de la estación de administración 69

Pasos de configuración de la estación de administración **69**

Requisitos de la red de la estación de administración **69**

Configuración de un explorador web admitido **70**

Abrir el explorador web. 70

Configuración del explorador web para conectarse a la interfaz web 70

Cómo agregar el iDRAC6 a la lista de dominios de confianza 74

Cómo ver las versiones traducidas de la interfaz web 75

Cómo establecer la configuración regional en Linux. 75

Desactivación de la función de lista blanca en Firefox 77

Instalación del software del iDRAC6 en la estación de administración **77**

Instalación y desinstalación de RACADM en una estación de administración. 78

Instalación y desinstalación de RACADM en Linux. 78

Instalación de Java Runtime Environment (JRE) **79**

Instalación de clientes Telnet o SSH **80**

Telnet con iDRAC6 80

Configuración de la tecla de retroceso para las sesiones de Telnet 80

SSH con iDRAC6 81

Instalación de un servidor TFTP **83**

Instalación de Dell OpenManage IT Assistant **83**

Instalación de Dell Management Console **84**

4 Configuración del servidor administrado 85

Instalación del software en el servidor administrado **85**

Configuración del servidor administrado para capturar la pantalla de último bloqueo **86**

Desactivación de la opción de reinicio automático de Windows **87**

5 Configuración del iDRAC6 Enterprise por medio de la interfaz web 89

Acceso a la interfaz web **90**

Inicio de sesión 90

Cierre de sesión 91

Uso de varias fichas y ventanas del explorador 91

Configuración del NIC del iDRAC6 . . . . . **92**

Configuración de los valores de VLAN, de IPMI y de red 92

Configuración del filtrado de IP y bloqueo de IP 97

Configuración de los sucesos de plataforma **99**

Configuración de filtros de sucesos de plataforma (PEF) 100

Configuración de capturas de sucesos de plataforma (PET) 100

Configuración de alertas por correo electrónico 101

Configuración de IPMI en la LAN **103**

Cómo agregar y configurar usuarios del iDRAC6 . . . . . **104**

Autentificación de la clave pública en el SSH 105

Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales **112**

Capa de sockets seguros (SSL). 113

Solicitud de firma de certificado (CSR) 114

Acceso al menú principal de SSL. 114

Generación de una nueva solicitud de firma de certificado. 115

Carga de un certificado de servidor 116

Cómo ver un certificado de servidor 117

Configuración y administración de los certificados de Microsoft Active Directory **117**

Configuración de Active Directory (esquema estándar y esquema ampliado) 118

Cómo ver un certificado de CA de Active Directory. 125

Activación o desactivación del acceso a la configuración local **126**

Activación del acceso a la configuración local 126

Desactivación del acceso a la configuración local 126

Configuración de los servicios del iDRAC6 . . . . . **126**

Actualización del firmware de iDRAC6 . . . . . **129**

Actualización del firmware del iDRAC6 por medio del CMC 131

Reversión del firmware del iDRAC6 131

6 Uso del servicio de directorio de iDRAC6 133

Uso del iDRAC6 con Microsoft Active Directory 133

Prerrequisitos para activar la autentificación de Active Directory para iDRAC6 135

Activación de SSL en un controlador de dominio 135

Mecanismos de autentificación compatibles de Active Directory 138

Generalidades del esquema ampliado de Active Directory 139

Extensiones de esquema de Active Directory 139

Descripción de las extensiones de esquema del iDRAC6 140

Descripción general de los objetos de Active Directory 140

Acumulación de privilegios con el esquema extendido 142

Configuración de Active Directory con esquema extendido para acceder al iDRAC6 143

Cómo extender el esquema de Active Directory 143

Instalación de la extensión de Dell para el complemento Usuarios y equipos de Active Directory 150

Cómo agregar usuarios y privilegios del iDRAC6 a Active Directory 151

Configuración de Active Directory de Microsoft con esquema extendido por medio de la interfaz web del iDRAC6. 154

Configuración de Active Directory con esquema extendido por medio de RACADM 157

Generalidades del esquema estándar de Active Directory **160**

Casos de dominio único y dominio múltiple . . . 161

Configuración de Active Directory con esquema estándar para acceder al iDRAC6 . . . . . **162**

Configuración de Active Directory con esquema estándar mediante la interfaz web del iDRAC6 162

Configuración de Active Directory con esquema estándar vía RACADM 166

Prueba de las configuraciones realizadas **169**

Cómo utilizar el iDRAC6 con el servicio de directorios LDAP **170**

Sintaxis de inicio de sesión (usuario de directorio y usuario local) 170

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web de iDRAC6. 171

Preguntas frecuentes **175**

Problemas de inicio de sesión en Active Directory. 175

Validación del certificado de Active Directory. 178

Esquema extendido y esquema estándar 179

Varios 180

7 Configuración de iDRAC6 para el inicio de sesión único y mediante tarjeta inteligente 181

Acerca de la autentificación basada en Kerberos. **181**

Prerrequisitos para el inicio de sesión único y la autentificación mediante tarjeta inteligente de Active Directory **182**

Uso de SSO de Active Directory **185**

Configuración del iDRAC6 para utilizar el inicio de sesión único 185

Inicio de sesión en iDRAC6 mediante inicio de sesión único 188

Configuración de la autentificación de tarjeta inteligente **189**

Configuración del Inicio de sesión mediante tarjeta inteligente en el iDRAC6 . . . . . **189**

Inicio de sesión en el iDRAC6 mediante la autentificación con tarjeta inteligente de Active Directory **191**

Preguntas frecuentes acerca del inicio de sesión único **191**

Solución de problemas de inicio de sesión mediante tarjeta inteligente en el iDRAC6 . . . . . **192**

8 Visualización de la configuración y la condición del servidor administrado . . . 195

System Summary (Resumen del sistema) **195**

Detalles del sistema **195**

Gabinete del sistema principal 195

Integrated Dell Remote Access Controller 6: Enterprise 197

WWN/MAC **200**

Condición del servidor **200**
iDRAC6 201
CMC 201
Baterías 201
Temperatures 202
Voltajes 202
Supervisión de alimentación 202
CPU 203
POST 203
Condiciones diversas 203

Inventario del sistema **203**
Solución de problemas 205

9 Configuración y uso de la comunicación en serie en la LAN 207

Activación de la comunicación en serie en la LAN del BIOS **207**

Configuración de la comunicación en serie en la LAN en la interfaz gráfica del usuario de web del iDRAC6 . . . . . **209**

Uso de la comunicación en serie en la LAN (SOL) **211**
Modelo para dirigir la comunicación en serie en la LAN a través de Telnet o SSH 211
Modelo para proxy SOL. 212
Modelo para dirigir la comunicación en serie en la LAN a través de IPMItool 212
Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6 212
Uso de SOL a través de PuTTY 213
Uso de la comunicación en serie en la LAN mediante Telnet con Linux 214

Uso de la comunicación en serie en la LAN mediante OpenSSH con Linux 214
Uso de SOL a través de IPMItool. 215
Ejecución de SOL con el proxy SOL 216

Configuración del sistema operativo **221**
Sistema operativo Linux Enterprise 221
Windows 2003 Enterprise. 227

10 Uso de la consola virtual de la interfaz gráfica de usuario 229

Descripción general **229**

Uso de la consola virtual **229**
Limpiar el caché del explorador 230
Resoluciones de pantalla y velocidades de actualización admitidas 231
Configuración de la estación de administración. 231
Configuración de la consola virtual y los medios virtuales en la interfaz web del iDRAC6 232
Cómo abrir una sesión de consola virtual 234
Vista previa de la consola virtual. 237

Uso de Video Viewer **237**
Sincronización de los apuntadores del mouse. . . . 242
Desactivación o activación de la consola local 243

Inicio de la consola virtual y de los medios virtuales de manera remota **244**
Formato de URL. 245
Situaciones de error habituales 245

Preguntas frecuentes **246**

11 Configuración de la tarjeta vFlash SD y administración de las particiones vFlash 253

Instalación de una tarjeta SD estándar o vFlash **254**

Extracción de una tarjeta SD estándar o vFlash 255

Configuración de una tarjeta SD estándar o vFlash utilizando racadm **257**

Cómo mostrar las propiedades de la tarjeta SD estándar o vFlash 257

Activación o desactivación de la tarjeta SD estándar o vFlash 258

Inicialización de la tarjeta SD estándar o vFlash 258

Obtención del último estado de la tarjeta SD estándar o vFlash 258

Restablecimiento de la tarjeta SD estándar o vFlash 258

Administración de las particiones vFlash mediante la interfaz web del iDRAC6 . . . . . **259**

Creación de una partición vacía 259

Creación de una partición utilizando un archivo de imagen 261

Formateo de una partición 263

Visualización de las particiones disponibles . . . 264

Modificación de una partición 266

Cómo conectar y desconectar una partición. . . . 266

Eliminación de las particiones existentes 268

Descarga del contenido de una partición 268

Inicio de una partición 269

Administración de particiones vFlash mediante racadm. **270**

Creación de una partición 271

Eliminación de una partición 272
Cómo obtener el estado de una partición 272
Visualización de la información de las particiones 272
Inicio de una partición 272
Conexión o desconexión de una partición 273
Modificación de una partición 273

Preguntas frecuentes **274**

12 Configuración y uso de medios virtuales 275

Descripción general **275**
Estación de administración basada en Windows 277
Estación de administración basada en Linux 278

Configuración de los medios virtuales **278**

Ejecución de los medios virtuales **280**
Desconexión de los medios virtuales 282
Inicio desde los medios virtuales. 282
Instalación de sistemas operativos mediante medios virtuales 283
Uso de medios virtuales cuando el sistema operativo del servidor está en ejecución 283

Preguntas frecuentes **284**

13 Uso de la interfaz de línea de comandos de RACADM 289

Subcomandos de RACADM **290**

Uso de comandos de RACADM local **293**

Uso de la utilidad RACADM para configurar el iDRAC6. . . . . **293**

Visualización de la configuración actual del iDRAC6 294

Administración de usuarios del iDRAC6 con RACADM 294

Cómo agregar un usuario del iDRAC6 295

Activación de un usuario del iDRAC6 con permisos 296

Carga, visualización y eliminación de claves SSH usando RACADM 297

Eliminación de un usuario del iDRAC6 298

Pruebas de las alertas por correo electrónico 298

Prueba de la función de alertas de capturas SNMP del iDRAC6. 299

Configuración de las propiedades de red del iDRAC6 299

Configuración de IPMI en la LAN. 301

Configuración del PEF 303

Configuración de la PET 303

Configuración del filtro de IP (Rango de IP) . . . 306

Configuración del bloqueo de IP 308

Configuración de los servicios de Telnet y SSH del iDRAC6 por medio de RACADM local . . . 311

RACADM SSH/Telnet y remoto. **312**

Uso de RACADM remoto 313

Opciones de RACADM remoto 314

Uso de un archivo de configuración de iDRAC6 . . . **314**

Creación de un archivo de configuración del iDRAC6 315

Sintaxis del archivo de configuración 315

Modificación de la dirección IP del iDRAC6 en un archivo de configuración 317
Carga del archivo de configuración en el iDRAC6 318

Configuración de varios iDRAC6 . . . . . **319**

14 Supervisión y administración de la alimentación 321

Configuración y administración de la alimentación **322**

Supervisión de alimentación **322**
Ver la supervisión de alimentación. 323

Presupuesto de alimentación **325**
Ver el presupuesto de alimentación 327
Umbral de presupuesto de alimentación. 328
Cómo ver y modificar la asignación de alimentación de PCIe 329

Power Control **330**
Ejecución de operaciones de control de alimentación en el servidor. 331

15 Uso de la interfaz de línea de comandos SM-C LP de iDRAC6 Enterprise 333

Administración del sistema por medio de SM-CLP . . . **334**

Compatibilidad con SM-CLP de iDRAC6 . . . . . **334**
Cómo iniciar una sesión SM–CLP 334

Funciones de SM-CLP **335**

Navegación en el espacio de direcciones de MAP **338**
Destinos 338

Uso del verbo show **338**
Uso de la opción -display 339
Uso de la opción -level 339
Uso de la opción -output 339

Ejemplos de SM-CLP del iDRAC6 . . . . . **340**
Administración de la alimentación del servidor 340
Administración de SEL 340
Navegación en MAP del destino 341

16 Uso de la interfaz WS-MAN 345

Funciones de WS-Management **345**

Perfiles CIM admitidos **346**

17 Implementación del sistema operativo por medio de iVMCLI 351

Antes de comenzar **351**
Requisitos del sistema remoto 351
Requisitos de red 351

Creación de un archivo de imagen de inicio **352**
Creación de un archivo de imagen para sistemas Linux 352
Creación de un archivo de imagen para sistemas Windows 352

Preparación para la implementación **352**
Configuración de sistemas remotos 352

Implementación del sistema operativo **353**

Uso de la utilidad de interfaz de línea de comandos de los soportes virtuales **355**
Instalación de la utilidad iVMCLI 356
Opciones de la línea de comandos. 356
Parámetros de iVMCLI 357
Opciones de shell de sistema operativo de iVMCLI 361

18 Uso de la utilidad de configuración del iDRAC6 363

Descripción general **363**

Inicio de la utilidad de configuración del iDRAC6 . . . . **364**

Uso de la utilidad de configuración del iDRAC6 . . . . **364**
LAN del iDRAC6. 365
IPMI en la LAN 366
Parámetros de la LAN 366
Configuración de soportes virtuales 370
Servicios del sistema. 372
Configuración de usuario de LAN 372
Restablecer valores predeterminados 375
Menú del registro de sucesos del sistema. 376
Cómo salir de la utilidad de configuración del iDRAC6 376

19 Recuperación y solución de problemas del sistema administrado 377

La seguridad primero, para el usuario y para el sistema **377**

Indicadores de problemas **378**

Indicadores LED. 378

Indicadores de problemas del hardware. 379

Otros indicadores de problemas 379

Herramientas para solución de problemas **380**

Consulta de la condición del sistema. 380

Consulta del registro de sucesos del sistema (SEL) 381

Verificar los códigos de la POST 383

Visualización de la pantalla de último bloqueo del sistema 383

Visualización de las secuencias de inicio más recientes. 384

Visualización y adición de notas de trabajo 385

Consulta de la pantalla de estado del servidor en busca de mensajes de error. 386

Visualización del registro del iDRAC6 396

Visualización de la información del sistema. . . . 397

Identificación del servidor administrado en el chasis. 398

Uso de la consola de diagnósticos 398

Administración de alimentación en un sistema remoto 400

Solución de problemas y preguntas frecuentes **402**

Índice 407

1

Descripción general del iDRAC6 Enterprise

Integrated Dell Remote Access Controller (iDRAC6) Enterprise es una solución de hardware y software de administración de sistemas que permite administración remota, recuperación de sistemas bloqueados y funciones de control de alimentación para los sistemas Dell PowerEdge.

iDRAC6 utiliza un microprocesador integrado de sistema en chip para el sistema remoto de control y supervisión y coexiste en la placa base con el servidor Dell PowerEdge administrado. El sistema operativo del servidor ejecuta programas de aplicación; iDRAC6 supervisa y administra el entorno y el estado del servidor fuera del sistema operativo.

Se puede configurar el iDRAC para que éste le envíe alertas por correo electrónico o alertas de captura de Protocolo simple de administración de red (SNMP) ante avisos o errores. Para ayudar a diagnosticar la causa de un bloqueo de sistema, iDRAC6 puede registrar datos de sucesos y capturar una imagen de la pantalla cuando detecta que el sistema se ha bloqueado.

Los servidores administrados están instalados en un gabinete (chasis) de sistema Dell M1000e con suministros de energía modulares, ventiladores de refrigeración y un Chassis Management Controller (CMC). El CMC supervisa y administra todos los componentes instalados en el chasis. Se puede agregar un CMC redundante para brindar protección contra fallas en caso de que el CMC principal falle. El chasis ofrece acceso a los dispositivos iDRAC6 por medio de la pantalla LCD, las conexiones de consola locales y la interfaz web. Cada módulo de alta densidad en un chasis tiene un iDRAC6. Puede instalar hasta 15 servidores blade en M1000e.

Todas las conexiones de red al iDRAC6 se enrutan a través de las interfaces de red del CMC (el puerto de conexión RJ45 del CMC etiquetado "GB1"). El CMC enruta el tráfico hacia los dispositivos iDRAC6 a través de una red privada interna. Esta red de administración privada está fuera de la ruta de acceso a datos del servidor y fuera del control del sistema operativo, es decir, está *fuera de banda*. Se puede acceder a las interfaces de red *dentro de banda* del servidor administrado mediante los módulos de E/S (IOM) instalados en el chasis.

NOTA: Se recomienda aislar o separar la red de administración del chasis, que es utilizada por el iDRAC6 y el CMC, de las redes de producción. Si se mezcla el tráfico de red de administración con el de producción o aplicación, existe la posibilidad de que la red se congestione o se sature, lo que puede causar demoras de comunicación del CMC y el iDRAC6. Las demoras pueden ocasionar un comportamiento impredecible del chasis, por ejemplo, que el CMC muestre que el iDRAC6 está fuera de línea a pesar de que funciona correctamente. Esto puede ocasionar un nuevo comportamiento impredecible.

De manera predeterminada, la interfaz de red del iDRAC6 está desactivada. Configure la interfaz de red del iDRAC6 antes de que se puede acceder a él. Una vez que el iDRAC6 esté activado y configurado en la red, se podrá tener acceso a él a través de la dirección IP asignada por medio de la interfaz web del iDRAC6, Telnet o SSH y de los protocolos de administración de red admitidos, como la Interfaz de administración de plataforma inteligente (IPMI).

Novedades de esta versión

- Compatibilidad para las configuraciones DIMM y tarjetas PCI (Para obtener más detalles consulte las Notas de la versión.)
- Compatibilidad para el explorador Internet Explorer 10.
- Configuración de correo electrónico de recurso a través de RACADM.
- Compatibilidad para la CPU AMD Abu Dhabi para M915, M910.

Certificación IPv6 Ready Logo

La misión del Comité de IPv6 Ready Logo es definir las especificaciones de prueba de cumplimiento e interoperabilidad de IPv6 para brindar acceso a herramientas de autoprueba y ofrecer IPv6 Ready Logo.

iDRAC6 cuenta con certificación **Fase 2 de IPv6 Ready Logo** y la identificación del logotipo es **02-C-000380**. Para obtener más información acerca del programa IPv6 Ready Logo, ver **URL ipv6ready.org/**.

Características de seguridad del iDRAC6

Las siguientes funciones se encuentran disponibles en el sistema de seguridad del iDRAC:

- Autentificación de usuarios por medio de Microsoft Active Directory, servicio de directorio de LDAP genérico o identificaciones y contraseñas de usuario administradas a nivel local
- Autentificación de dos factores proporcionada por la función de inicio de sesión con tarjeta inteligente. La autentificación de dos factores se basa en lo que los usuarios *tienen* (tarjeta inteligente) y lo que *conocen* (PIN).
- Autorización en base a funciones, que permite que el administrador configure privilegios específicos para cada usuario
- Configuración de la identificación y contraseña del usuario
- Las interfaces web y SM-CLP que son compatibles con los cifrados de 128 bits y 40 bits (para países en los que no se aceptan 128 bits), utilizando el estándar SSL 3.0
- Configuración del tiempo de espera de la sesión (en segundos)
- Puertos IP que se pueden configurar (si corresponde)
- Secure Shell (SSH), que usa una capa de transporte cifrado para ofrecer mayor seguridad
- Límites de falla de inicio de sesión por dirección IP, con bloqueo del inicio de sesión de la dirección IP cuando se ha superado el límite
- Rango configurable de direcciones IP para clientes que se conectan al iDRAC6

iDRAC6 Enterprise y tarjeta multimedia vFlash

iDRAC6 Enterprise dispone de ranuras de tarjeta SD para el soporte vFlash. Para obtener más información acerca del iDRAC6 Enterprise y el soporte vFlash, consulte el *Manual del propietario de hardware* en **dell.com/support/manuals**.

La Tabla 1-1 enumera las funciones disponibles para iDRAC6 Enterprise y el soporte vFlash.

Tabla 1-1. Lista de funciones del iDRAC6

Función	iDRAC6 Enterprise	iDRAC6 Enterprise con tarjeta multimedios vFlash
Compatibilidad con interfaces y estándares		
IPMI 2.0	✓	✓
Web GUI	✓	✓
SNMP	✓	✓
WS–MAN	✓	✓
SM-CLP	✓	✓
Línea de comandos RACADM	✓	✓
Conectividad		
Modos de red compartida/con protección contra fallas	✓	✓
IPv4	✓	✓
VLAN Tagging (Etiquetado VLAN)	✓	✓
IPv6	✓	✓
DNS dinámico	✓	✓
NIC dedicado	✓	✓

Tabla 1-1. Lista de funciones del iDRAC6 *(continuación)*

Función	iDRAC6 Enterprise	iDRAC6 Enterprise con tarjeta multimedios vFlash
Seguridad y autentificación		
Autorización basada en funciones	✓	✓
Local Users	✓	✓
Active Directory	✓	✓
Autentificación de dos factores	✓	✓
Inicio de sesión único	✓	✓
Cifrado SSL	✓	✓
Corrección y administración remota		
Actualización remota de firmware	✓	✓
Control de alimentación de servidor	✓	✓
Comunicación en serie en la LAN (con proxy)	✓	✓
Comunicación en serie en la LAN (sin proxy)	✓	✓
Power Capping (Límites de alimentación)	✓	✓
Captura de pantalla de último bloqueo	✓	✓
Captura de inicio	✓	✓
Medios virtuales	✓	✓
Recurso compartido de archivos remotos	✓	✓
Consola virtual	✓	✓
Consola virtual de uso compartido	✓	✓
vFlash	✗	✓

Tabla 1-1. Lista de funciones del iDRAC6 *(continuación)*

Función	iDRAC6 Enterprise	iDRAC6 Enterprise con tarjeta multimedios vFlash
Supervisión		
Alerta y supervisión de sensor	✓	✓
Supervisión de alimentación en tiempo real	✓	✓
Gráficos de alimentación en tiempo real	✓	✓
Medidores de datos históricos de alimentación	✓	✓
Inventario del sistema	✓	✓
Registro		
Registro de sucesos del sistema (SEL)	✓	✓
Registro del RAC	✓	✓
Registro de rastreo	✓	✓
Registro del sistema remoto	✓	✓
Notas de trabajo	✓	✓

✓ = compatible; ✗ = no compatible

Plataformas admitidas

Para conocer las plataformas compatibles más recientes, consulte el archivo léame del iDRAC6 y la *Dell Systems Software Support Matrix* (Matriz de compatibilidad de software de sistemas Dell) disponible en **dell.com/support/manuals**.

Sistemas operativos compatibles

Para obtener la información más actualizada, consulte el archivo Léame del iDRAC6 y la *Dell Systems Software Support Matrix* (Matriz de compatibilidad de software de los sistemas Dell) que se encuentra disponible en **dell.com/support/manuals**.

Exploradores web admitidos

Para obtener la información más actualizada, consulte el archivo léame y la *Dell Systems Software Support Matrix* (Matriz de compatibilidad de software de los sistemas Dell) que se encuentra disponible en **dell.com/support/manuals**.

NOTA: La compatibilidad con SSL 2.0 se interrumpió debido a defectos de seguridad. Asegúrese de que el explorador esté configurado para activar SSL 3.0.

Conexiones de acceso remoto admitidas

La Tabla 1-2 muestra una lista de las funciones de conexión.

Tabla 1-2. Conexiones de acceso remoto admitidas

Conexión	Características
Tarjeta de interfaz de red del iDRAC6	• Ethernet de 10 Mbps/100 Mbps/1 Gbps a través del puerto Gb Ethernet del CMC. • Compatibilidad con DHCP. • Notificación de sucesos por correo electrónico y capturas SNMP. • Los comandos de RACADM y shell de SM–CLP para operaciones como configuración del iDRAC6, los comandos de inicio, restablecimiento, encendido y apagado del sistema son admitidos a través de SSH y Telnet. • Compatibilidad para las utilidades de IPMI, como IPMItool e ipmish.

Puertos del iDRAC6

La Tabla 1-3 muestra una lista de los puertos en los que el iDRAC6 detecta las conexiones.La Tabla 1-4 identifica los puertos que el iDRAC6 utiliza como cliente. Esta información es necesaria cuando se abren servidores de seguridad para permitir el acceso remoto a un iDRAC6.

PRECAUCIÓN: iDRAC6 no verifica si hay conflictos entre los puertos configurables. Al establecer las configuraciones de los puertos, verifique que las asignaciones de puertos no entren en conflicto unas con otras.

Tabla 1-3. Puertos en los que el iDRAC6 detecta servidores

Port Number (Número de puerto)	Función
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668, 3669	Servicio de medios virtuales
3670, 3671	Servicio seguro de medios virtuales
5900*	Teclado/mouse de consola virtual
5901*	Vídeo de consola virtual
5988	Utilizado para WSMAN

* Puerto configurable

Tabla 1-4. Puertos de cliente del iDRAC6

Port Number (Número de puerto)	Función
25	SMTP
53	DNS
68	Dirección IP asignada por DHCP
69	TFTP

Tabla 1-4. Puertos de cliente del iDRAC6 *(continuación)*

Port Number (Número de puerto)	Función
162	Captura SNMP
636	LDAPS
3269	LDAPS para catálogo global (GC)

Otros documentos que podrían ser útiles

Además de esta guía, los siguientes documentos, disponibles en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**, proporcionan información adicional acerca de la configuración y la operación del iDRAC6 en su sistema.

- La ayuda en línea para el iDRAC6 proporciona información acerca del uso de la interfaz web.
- La *Dell Chassis Management Controller User Guide* (Guía del usuario de Dell Chassis Management Controller) suministra información acerca del uso de la controladora que administra todos los módulos en el chasis que contienen su servidor Dell PowerEdge.
- La *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller) brinda información acerca de Unified Server Configurator (USC), Unified Server Configurator: Lifecycle Controller Enabled (USC – LCE) y servicios remotos.
- Los documentos *iDRAC6 CIM Element Mappings (Asignación de elementos CIM del iDRAC6)* y *iDRAC6 SM-CLP Property Database* (Base de datos de propiedades del iDRAC6 SM-CLP), disponibles en el Dell Enterprise Technology Center en **delltechcenter.com**, brindan información sobre la base de datos de propiedades del iDRAC6 SM–CLP, la asignación entre clases WS–MAN y destinos SM–CLP y los detalles de implementación de Dell.
- La *Dell RACADM Command Line Reference Guide for iDRAC6 and CMC* (Guía de referencia de la línea de comandos de RACADM para iDRAC6 y CMC) proporciona información sobre los subcomandos RACADM, las interfaces RACADM admitidas, los grupos de base de datos de propiedades y las definiciones de objetos para iDRAC6 Enterprise en servidores blade, iDRAC6 Enterprise o Express en servidores de torre o estante y CMC.

- La *Matriz de compatibilidad de software de sistemas Dell* ofrece información sobre los diversos sistemas Dell, los sistemas operativos compatibles con esos sistemas y los componentes de Dell OpenManage que se pueden instalar en estos sistemas.
- La *Guía de instalación de Dell OpenManage Server Administrator* contiene instrucciones para ayudarlo a instalar Dell OpenManage Server Administrator.
- La *Guía de instalación de Dell OpenManage Management Station Software* contiene instrucciones para ayudarlo a instalar este software que incluye la utilidad de administración de la placa base, herramientas de DRAC y el complemento de Active Directory.
- La *Dell Management Console User's Guide* (Guía del usuario de la consola de administración Dell) ofrece información acerca del uso de la consola de administración Dell.
- La *Dell OpenManage Server Administrator User's Guide* (Guía del usuario de Server Administrator de Dell OpenManage) contiene información acerca de la instalación y el uso de Server Administrator.
- La *Dell Update Packages User's Guide* (Guía del usuario de Dell Update Packages) contiene información acerca de cómo obtener y utilizar los paquetes Dell Update Packages como parte de su estrategia de actualización del sistema.
- El *Glosario* proporciona información acerca de los términos utilizados en este documento.

Los siguientes documentos del sistema también están disponibles para proporcionar más información acerca del sistema en el que iDRAC6 está instalado:

- En las instrucciones de seguridad incluidas con el sistema se proporciona información importante sobre normativas y seguridad. Para obtener más información sobre normativas, consulte la página principal de Cumplimiento de normativas en **dell.com/regulatory_compliance**. La información sobre la garantía puede estar incluida en este documento o constar en un documento aparte.
- En la *Guía de introducción* se proporciona información general sobre las características del sistema, la configuración del sistema y las especificaciones técnicas.

- En el *Manual del propietario de hardware*, se proporciona información acerca de las funciones del sistema y se describe cómo solucionar problemas del sistema e instalar o sustituir componentes.
- En la documentación del software de administración de sistemas se describen las características, los requisitos, la instalación y el funcionamiento básico del software.
- En la documentación del sistema operativo se describe cómo instalar (si es necesario), configurar y utilizar el software del sistema operativo.
- En la documentación de los componentes adquiridos por separado se incluye información para configurar e instalar las opciones correspondientes.
- Algunas veces, con el sistema se incluyen actualizaciones que describen los cambios realizados en el sistema, en el software o en la documentación.

  NOTA: Lea siempre las actualizaciones primero, puesto que a menudo sustituyen la información contenida en otros documentos.
- Se incluyen Notas de la versión o archivos Léame para proporcionar actualizaciones de última hora relativas al gabinete o la documentación, o material de consulta técnica avanzada destinado a técnicos o usuarios experimentados.

Acceso a los documentos desde el sitio web del servicio de asistencia Dell Support

Para acceder a los documentos desde el sitio web del servicio de asistencia Dell Support

1. Vaya a **dell.com/support/manuals**.
2. En la sección **Información sobre su sistema Dell**, en **No**, seleccione **Elegir de una lista de todos los productos Dell** y haga clic en **Continuar**.
3. En la sección **Seleccione su tipo de producto**, haga clic en **Software, supervisores, productos electrónicos y periféricos**.
4. En la sección **Elija software, supervisores, productos electrónicos y periféricos Dell**, haga clic en **Software**.
5. En la sección **Elija su software Dell**, haga clic en el vínculo requerido que corresponda:

- Client System Management
- Enterprise System Management
- Remote Enterprise System Management
- Herramientos de servicio

6 Para ver el documento, haga clic en la versión del producto requerida.

También puede acceder directamente a los documentos con los siguientes vínculos:

- Para documentos de Client System Management: **dell.com/OMConnectionsClient**
- Para documentos de Enterprise System Management: **dell.com/openmanagemanuals**
- Para documentos de Remote Enterprise System Management: **dell.com/openmanagemanuals**
- Para documentos de Herramientas de servicio: **dell.com/serviceabilitytools**

2

Configuración de iDRAC6 Enterprise

Esta sección contiene información acerca de cómo establecer el acceso al iDRAC6 y configurar el entorno de administración para utilizarlo.

Antes de comenzar

Reúna los siguientes elementos antes de configurar el iDRAC6:

- *Guía del usuario del firmware de Dell Chassis Management Controller*
- DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell systems Management)

El DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell systems Management) incluye los siguientes componentes:

- Directorio raíz del DVD: contiene Dell Systems Build and Update Utility, que proporciona información acerca de la configuración del servidor y de instalación del sistema.
- SYSMGMT: contiene productos de software de administración de sistemas, incluso Dell OpenManage Server Administrator

Para obtener más información, consulte la *Dell OpenManage Server Administrator Installation Guide* (Guía de instalación de Dell OpenManage Server Administrator) y la *Dell OpenManage Management Station Software Installation Guide* (Guía de instalación de Dell OpenManage Management Station Software) disponibles en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Interfaces para configurar el iDRAC6

Puede configurar el iDRAC6 mediante la utilidad de configuración del iDRAC6, la interfaz web del iDRAC6, la interfaz web de Chassis Management Controller (CMC), el panel LCD del chasis, la interfaz de línea de comandos de RACADM local o remoto, iVMCLI o la interfaz de línea de comandos de SM-CLP. La CLI de RACADM local está disponible después haber instalado el sistema operativo y el software Dell OpenManage en el servidor administrado. La Tabla 2-1 describe estas interfaces.

Para obtener mayor seguridad, acceda a la configuración del iDRAC6 a través de la Utilidad de configuración del iDRAC6 o desactive la CLI de RACADM local mediante un comando RACADM (consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* [Guía de referencia de la línea de comandos RACADM para iDRAC y CMC] disponible en **dell.com/support/manuals**) o desde la GUI (ver "Activación o desactivación del acceso a la configuración local" en la página 126.)

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

Tabla 2-1. Interfaces de configuración

Interfaz	Descripción
Configuración del iDRAC6 Utilidad	Se accede a la utilidad de configuración del iDRAC6 al momento del inicio, y es una herramienta útil cuando se instala un nuevo servidor Dell PowerEdge. Úsela para configurar la red y las funciones básicas de seguridad, así como para activar otras funciones.
Interfaz web del iDRAC6	La interfaz web del iDRAC6 es una aplicación de administración a la que se accede por medio de un explorador y que se puede utilizar para administrar el iDRAC6 de manera interactiva y supervisar el servidor administrado. Es la interfaz principal para las tareas cotidianas, como la supervisión de la condición de sistema, la consulta del registro de sucesos del sistema, la administración de usuarios locales del iDRAC6 y la ejecución de la interfaz web del CMC y las sesiones de consola virtual.
Interfaz web del CMC	Además de supervisar y administrar el chasis, la interfaz web del CMC se puede utilizar para ver el estado de un servidor administrado, actualizar el firmware del iDRAC6, establecer la configuración de la red del iDRAC6, iniciar sesión en la interfaz web del iDRAC6 e iniciar, detener o restablecer el servidor administrado.

Tabla 2-1. Interfaces de configuración *(continuación)*

Interfaz	Descripción
Panel LCD del chasis	El panel LCD en el chasis que contiene el iDRAC6 se puede utilizar para ver el estado general de los servidores en el chasis. Durante la configuración inicial del CMC, el asistente de configuración permite activar la configuración de DHCP del sistema de red del iDRAC6.
RACADM local y remoto	La interfaz de línea de comandos de RACADM local se ejecuta en el servidor administrado. RACADM remoto es una utilidad cliente que se ejecuta en una estación de administración. Utiliza una interfaz de red fuera de banda para ejecutar comandos de RACADM en el servidor administrado. La opción **–r** ejecuta el comando de RACADM en una red. Los comandos de RACADM proporcionan acceso a casi todas las funciones de iDRAC6. Usted puede inspeccionar datos de sensor, anotaciones del registro de sucesos del sistema, el estado actual y los valores de configuración que se mantienen en el iDRAC6. También puede cambiar los valores de configuración del iDRAC6, administrar usuarios locales, activar y desactivar funciones y realizar acciones de alimentación como apagar o reiniciar el servidor administrado.
iVMCLI	La interfaz de línea de comandos de medios virtuales del iDRAC6 (iVMCLI) proporciona al servidor administrado acceso a los medios que se encuentran en la estación de administración. Es útil para desarrollar secuencias de comandos para instalar sistemas operativos en varios servidores administrados.

Tabla 2-1. Interfaces de configuración *(continuación)*

Interfaz	Descripción
SM-CLP	SM-CLP es la implementación incorporada en el iDRAC6 del Protocolo de línea de comandos de administración de servidor (SM-CLP) del grupo de trabajo de administración de servidor. A la línea de comandos de SM-CLP se accede iniciando sesión en el iDRAC6 a través de Telnet o SSH y escribiendo `smclp` en la petición de la interfaz de línea de comandos. Los comandos de SM-CLP implementan un subconjunto útil de los comandos de RACADM local. Los comandos son útiles para la creación de secuencias de comandos ya que los puede ejecutar desde una línea de comandos de la estación de administración. La salida de los comandos se puede obtener en formatos bien definidos, incluso en XML, lo que facilita la creación de secuencias de comandos y la integración con las herramientas de informes y de administración existentes.
IPMI	IPMI define una manera estándar en la que los subsistemas de administración incorporados, como el iDRAC6, se comunican con otros sistemas incorporados y aplicaciones de administración. Usted puede utilizar la interfaz web del iDRAC6, SM-CLP o los comandos de RACADM para configurar filtros de sucesos de plataforma (PEF) de IPMI y capturas de sucesos de plataforma (PET). Los filtros de sucesos de plataforma hacen que el iDRAC6 realice acciones específicas (por ejemplo, que reinicie el servidor administrado) cuando detecta una condición. Las capturas de sucesos de plataforma indican al iDRAC6 que envíe correo electrónico o alertas de IPMI cuando detecta los sucesos o condiciones especificados. También puede utilizar herramientas IPMI estándares como **IPMItool** e **ipmish** con iDRAC6 cuando activa IPMI en la LAN.

Tareas de configuración

Esta sección ofrece una descripción general de las tareas de configuración de la estación de administración, el iDRAC6 y el servidor administrado. Entre las tareas que se pueden llevar a cabo se incluyen la configuración del iDRAC6 para acceso remoto, la configuración de las funciones del iDRAC6 que desea utilizar, la instalación del sistema operativo en el servidor administrado y la instalación del software de administración en la estación de administración y el servidor administrado.

Las tareas de configuración necesarias para realizar cada tarea se encuentran en la parte inferior de la tarea.

NOTA: Antes de realizar los procedimientos de configuración de esta guía, instale CMC y los módulos de E/S del chasis y configure, e instale físicamente el servidor Dell PowerEdge en el chasis.

Configurar la estación de administración

Establezca una estación de administración mediante la instalación del software Dell OpenManage, un explorador web y otras utilidades de software. Vea la "Configuración de la estación de administración" en la página 69.

Configurar el sistema de red del iDRAC6

Active la red del iDRAC6 y configure las direcciones IP, la máscara de red, la puerta de enlace y las direcciones DNS.

NOTA: Acceda a la configuración del iDRAC6 a través de la Utilidad de configuración del iDRAC6 o desactive la CLI de RACADM local mediante un comando RACADM (consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* [Guía de referencia de la línea de comandos RACADM para iDRAC y CMC] disponible en **dell.com/support/manuals**) o desde la GUI (ver "Activación o desactivación del acceso a la configuración local" en la página 126.)

NOTA: Si cambia la configuración de la red del iDRAC6, cerrará todas las conexiones actuales de red al iDRAC6.

NOTA: La opción para configurar el servidor mediante el panel LCD *sólo* está disponible durante la configuración inicial del CMC. Una vez que el chasis ha sido implementado, no puede reconfigurar el iDRAC6 utilizando el panel LCD.

NOTA: Utilice el panel LCD solamente para activar DHCP para configurar la red del iDRAC6.

- Panel LCD del chasis: consulte la *Dell Chassis Management Controller Firmware User Guide* (Guía del usuario de firmware de Dell Chasis Management Controller).
- Utilidad de configuración del iDRAC6: ver "Uso de la utilidad de configuración del iDRAC6" en la página 363.
- Interfaz web del CMC: ver "Configuración de la red por medio de la interfaz web del CMC" en la página 42
- RACADM local y remoto: consulte **cfgLanNetworking** en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en **dell.com/support/manuals**.

Configurar los usuarios de iDRAC6

Configure los usuarios y permisos locales del iDRAC6. El iDRAC6 contiene una tabla de dieciséis usuarios locales en el firmware. Usted puede establecer nombres de usuarios, contraseñas y funciones para estos usuarios.

- Utilidad de configuración del iDRAC6 (sólo configura al usuario administrativo): ver "Configuración de usuario de LAN" en la página 372
- Interfaz web del iDRAC6: ver "Cómo agregar y configurar usuarios del iDRAC6" en la página 104
- RACADM local y remoto: ver "Cómo agregar un usuario del iDRAC6" en la página 295

NOTA: Al utilizar el iDRAC6 en un entorno de servicio de directorios de Active Directory/LDAP genérico, asegúrese de que los nombres de usuario cumplan con la convención vigente del servicio de directorios de Active Directory/LDAP genérico.

Configurar servicios de directorios

Además de los usuarios locales de iDRAC6, puede utilizar Microsoft Active Directory o un servicio de directorio LDAP genérico para autenticar los inicios de sesión de los usuarios de iDRAC6.

Para obtener más información, consulte "Uso del servicio de directorio de iDRAC6" en la página 133.

Configurar la filtración y el bloqueo de IP

Además de la autentificación de usuario, usted puede impedir los accesos no autorizados mediante el rechazo de los intentos de conexión de direcciones IP fuera de un rango definido y mediante el bloqueo temporal de las conexiones de direcciones IP donde la autentificación ha fallado varias veces dentro de un periodo configurable.

- Interfaz de web del iDRAC6: ver "Configuración del filtrado de IP y bloqueo de IP" en la página 97.
- RACADM: ver "Configuración del filtro de IP (Rango de IP)" en la página 306 y "Configuración del bloqueo de IP" en la página 308.

Configurar los sucesos de plataforma

Los sucesos de plataforma ocurren cuando el iDRAC6 detecta una condición de aviso o crítica de uno de los sensores del servidor administrado.

Configure los filtros de sucesos de plataforma (PEF) para elegir las acciones que desea ejecutar, por ejemplo, el reinicio del servidor administrado, cuando se detecta un suceso.

- Interfaz web del iDRAC6: ver "Configuración de filtros de sucesos de plataforma (PEF)" en la página 100.
- RACADM: ver "Configuración del PEF" en la página 303.

Configure capturas de sucesos de plataforma (PET) para enviar notificaciones de alerta a una dirección IP, por ejemplo, a una estación de administración con el software de administración o para enviar un correo electrónico a una dirección de correo electrónico específica.

- Interfaz web del iDRAC6: ver "Configuración de capturas de sucesos de plataforma (PET)" en la página 100.
- RACADM: ver "Configuración de la PET" en la página 303.

Activación o desactivación del acceso a la configuración local

El acceso a los parámetros de configuración críticos como la configuración de la red y los privilegios de usuario puede desactivarse. Una vez desactivado, la configuración persiste al reiniciar. El acceso de escritura de configuración está bloqueado tanto para el programa RACADM local como para la utilidad de configuración del iDRAC6 (al iniciar). El acceso web a los parámetros de configuración está libre y los datos de configuración siempre están disponibles para su visualización. Para obtener más información acerca de la interfaz web iDRAC6, ver "Activación o desactivación del acceso a la configuración local" en la página 126. Para los comandos de RACADM, consulte **cfgRacTuning** en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en **dell.com/support/manuals**.

Configurar los servicios del iDRAC6

Active o desactive los servicios de red del iDRAC6 (como Telnet, SSH y la interfaz de Web Server) y reconfigure los puertos y otros parámetros de servicio.

- Interfaz web del iDRAC6: ver "Configuración de los servicios del iDRAC6" en la página 126
- RACADM: ver "Configuración de los servicios de Telnet y SSH del iDRAC6 por medio de RACADM local" en la página 311

Configurar la capa de sockets seguros (SSL)

Configurar SSL para el servidor web del iDRAC6.

- Interfaz web del iDRAC6: ver "Capa de sockets seguros (SSL)" en la página 113
- RACADM: consulte cfgRacSecurity, sslcsrgen, sslcertupload, sslcertdownload, y sslcertview en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Configurar los medios virtuales

Configure la función de medios virtuales para que pueda instalar el sistema operativo en el servidor Dell PowerEdge. Los medios virtuales permiten que el servidor administrado tenga acceso a dispositivos de medios en la estación de administración o a imágenes ISO de CD/DVD que estén en un recurso compartido de red como si fueran dispositivos en el servidor administrado.

- Interfaz web del iDRAC6: ver "Configuración y uso de medios virtuales" en la página 275
- Utilidad de configuración del iDRAC6: Consulte "Configuración de soportes virtuales" en la página 370

Configurar una tarjeta multimedios vFlash

Instalar y configurar una tarjeta multimedios vFlash para utilizarla con iDRAC6.

- Interfaz web del iDRAC6 y uso de RACADM: ver "Configuración de la tarjeta vFlash SD y administración de las particiones vFlash" en la página 253

Instalación del software de servidor administrado

Instale el sistema operativo en el servidor Dell PowerEdge mediante los medios virtuales, luego instale el software Dell OpenManage en el servidor Dell PowerEdge administrado y configure la función de pantalla de último bloqueo.

- Consola virtual: ver "Instalación del software en el servidor administrado" en la página 85
- iVMCLI: ver "Uso de la utilidad de interfaz de línea de comandos de los soportes virtuales" en la página 355

Configure el servidor administrado para utilizar la función de pantalla de último bloqueo

Configure el servidor administrado de modo que el iDRAC6 pueda capturar la imagen de la pantalla tras un bloqueo o falla general del sistema operativo.

- Servidor administrado: ver "Configuración del servidor administrado para capturar la pantalla de último bloqueo" en la página 86 y "Desactivación de la opción de reinicio automático de Windows" en la página 87

Configuración de la red por medio de la interfaz web del CMC

NOTA: Debe contar con privilegios de administrador de configuración del chasis para definir la configuración de la red de iDRAC6 desde CMC.

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

Iniciar la interfaz web del iDRAC6 desde el CMC

El CMC proporciona administración limitada de componentes individuales del chasis, tales como servidores. Para la administración completa de estos componentes individuales, el CMC proporciona un punto de inicio para la interfaz web del iDRAC6 del servidor.

Para iniciar el iDRAC6 desde el CMC:

1. Inicie sesión en la interfaz web del CMC.
2. En el árbol del sistema, seleccione **Información general del servidor**. La pantalla **Estado de los servidores** muestra la lista de servidores disponibles.
3. Haga clic en el **iDRAC** para el servidor que desea administrar. Se inicia la interfaz gráfica del usuario del iDRAC en una ventana de explorador nueva.

Para iniciar la interfaz web del iDRAC6 para un solo servidor desde el CMC.

1. Inicie sesión en la interfaz web del CMC.
2. Expanda la opción **Descripción general de servidores** en el árbol del sistema. Todos los servidores aparecen en la lista ampliada de **Servidores**.
3. Haga clic en el servidor que desea ver. Aparece la pantalla **Estado del servidor** para el servidor que seleccionó.
4. Haga clic en **Iniciar la interfaz gráfica de usuario de iDRAC6**.

Inicio de sesión único

Con la función de inicio de sesión único, puede abrir la interfaz web del iDRAC6 desde el CMC sin tener que iniciar sesión por segunda vez. Las políticas de inicio de sesión único se describen a continuación.

- Un usuario del CMC con **Server Administrator** configurado en **Privilegios de usuario** se conecta automáticamente con la interfaz web del iDRAC6 mediante el inicio de sesión único. Después de iniciar sesión, se otorgan privilegios de administrador del iDRAC6 al usuario. Esto sucede aunque éste no tenga una cuenta en iDRAC6 o si la cuenta no tiene privilegios de administrador.
- Un usuario de CMC que no tenga **Server Administrator** configurado en **Privilegios de usuario** pero con la misma cuenta en iDRAC6, se conecta automáticamente con iDRAC6 mediante un inicio de sesión único. Una vez conectado a la interfaz web del iDRAC6, se otorgan a este usuario privilegios creados para la cuenta iDRAC6.

  NOTA: En este contexto, *la misma cuenta* significa que el usuario tiene el mismo nombre de usuario y contraseña para CMC y para iDRAC6. Un usuario que tiene el mismo nombre usuario pero una contraseña diferente no es reconocido como un usuario válido.
- Un usuario de CMC que no tenga **Server Administrator** configurado en **Privilegios de usuario** o la misma cuenta en iDRAC6 *no* se conecta automáticamente con iDRAC6 mediante el inicio de sesión único. Este usuario será dirigido a la página de inicio de sesión del iDRAC6 luego de hacer clic en **Iniciar interfaz gráfica de usuario del iDRAC6**.

  NOTA: Si se desactiva la LAN de la red del iDRAC6 (LAN activada = No), el inicio de sesión único no estará disponible.

  NOTA: Si se extrae el servidor del chasis, se cambia la dirección IP del iDRAC6 o la conexión de red del iDRAC6 tiene algún problema, al hacer clic en el icono **Iniciar interfaz gráfica de usuario del iDRAC6** puede aparecer una pantalla de error.

Configuración de la conexión de red de iDRAC6

1. Haga clic en **Sistema→ Configuración de iDRAC→ ficha Red/Seguridad**.
2. Para activar o desactivar la comunicación en serie en la LAN:
   a. Haga clic en **Comunicación en serie en la LAN**.

      Se muestra la pantalla **Comunicación en serie en la LAN**.

b Seleccione la casilla de verificación **Activar comunicación en serie en la LAN**. También puede cambiar la configuración de **Velocidad en baudios** y **Límite de nivel de privilegio del canal**.

c Haga clic en **Aplicar**.

3 Para activar o desactivar IPMI en la LAN:

a Haga clic en **Network** (Red).

Se muestra la pantalla **Red**.

b Haga clic en **Configuración de IPMI**.

c Seleccione la casilla de verificación **Activar IPMI en la LAN**. También puede cambiar la configuración de **Límite de nivel de privilegio del canal** y **Clave de cifrado**.

d Haga clic en **Aplicar**.

4 Para activar o desactivar DHCP:

a Haga clic en **Network** (Red).

Se muestra la pantalla **Red**.

b En la sección **Configuración de IPv4**, seleccione las casillas de verificación **Activación de DHCP** y **Usar DHCP para obtener las direcciones del servidor DNS**.

c En la sección **Configuración de IPv6**, seleccione las casillas de verificación **Activación de configuración automática** y **Utilizar DHCPv6 para obtener las direcciones del servidor DNS**.

d Haga clic en **Aplicar**.

NOTA: Si decide no activar DHCP, debe introducir la dirección IP estática, la máscara de red y la puerta de enlace predeterminada del servidor.

Visualización de las conexiones de red Fabric de la tarjeta mezzanine FlexAdress

El M1000e incluye FlexAdress, un sistema de red multiestándar avanzado de varios niveles. FlexAddress permite el uso de nombres de red mundial y direcciones MAC (WWN/MAC) persistentes con chasis asignado para cada conexión de puerto de servidor administrada.

NOTA: Con el propósito de evitar errores que puedan impedir el encendido en el servidor administrado, se *debe* tener el tipo correcto de tarjeta mezzanine para cada conexión de puerto y de red Fabric.

La configuración de la función FlexAddress se realiza utilizando la interfaz web de CMC. Para obtener más información acerca de la función FlexAddress y su configuración, consulte la *Dell Chassis Management Controller User Guide* (Guía del usuario de Dell Chassis Management Controller) y el documento *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* (Especificaciones técnicas de la tarjeta Secure Digital (SD) de Chassis Management Controller [CMC])

Una vez que la función FlexAddress se ha activado y configurado para el chasis, haga clic en **Sistema**→ ficha **Propiedades**→ **WWN/MAC** para ver una lista de las tarjetas mezzanine instaladas, las redes Fabric a las que están conectadas, el tipo de red Fabric y las direcciones MAC asignadas por el servidor o chasis para cada puerto de tarjeta mezzanine opcional y Ethernet incorporado que se haya instalado.

La columna **Asignadas por el servidor** muestra las direcciones WWN/MAC asignadas por el servidor que están incorporadas al hardware del controlador. Las direcciones WWN/MAC que muestran el texto **N/A** indican que no se ha instalado una interfaz para la red Fabric especificada.

La columna **Asignadas por el chasis** muestra las direcciones WWN/MAC asignadas por el chasis que se utilizan para una ranura en particular. Las direcciones WWN/MAC que muestran el texto **N/A** indican que no se ha instalado la función FlexAddress.

La columna **Asignadas de manera remota** muestra la dirección WWN/MAC asignada por el usuario a través de WSMAN. Solamente se muestra si la opción FlexAddress está desactivada y la administración remota se encuentra activada. Consulte la *Dell Lifecycle Controller User's Guide* (Guía del usuario de Dell Lifecycle Controller) y *iDRAC6 CIM Element Mappings* (Aignación de elementos CIM del iDRAC6) para obtener más información.

Una marca de verificación en las columnas **Asignadas por el servidor**, **Asignadas por el chasis**, y **Asignadas de manera remota** indica las direcciones activas.

Cuando la dirección flex del chasis se encuentra activa, la GUI del iDRAC muestra la dirección MAC asignada de CMC y la dirección MAC no asignada remotamente. Se muestra la dirección MAC asignada por el servidor pero no es activa.

Cuando las direcciones MAC asignadas remotamente son activas, la página de la interfaz web de CMC muestra la dirección MAC como administrada remotamente para una ranura particular en el chasis.

Solamente se muestran las direcciones asignadas remotamente en la GUI Fuera de banda (OOB) del iDRAC y no por medio de otras interfaces como RACADM y las herramientas IPMI.

Dirección MAC de FlexAddress para iDRAC6

La función FlexAddress reemplaza las direcciones MAC asignadas por el servidor por direcciones MAC asignadas por el chasis y se implementa para el iDRAC6 junto con LOM de módulos de alta densidad, tarjetas mezzanine y módulos de E/S. La función FlexAddress del iDRAC6 admite la preservación de la dirección MAC específica de una ranura para los iDRAC6 en un chasis. La dirección MAC asignada por el chasis se almacena en la memoria no volátil y se envía al iDRAC6 durante su proceso de inicio o al cambiar la configuración en la página C MC FlexAddress.

Si el CMC activa la dirección MAC asignada por el chasis, el iDRAC6 mostrará el valor en el campo **Dirección MAC** en las siguientes pantallas:

- **Sistema**→ ficha **Propiedades**→ **Detalles del sistema**→ **Información del iDRAC6**
- **Sistema**→ ficha **Propiedades**→ **WWN/MAC**
- **Sistema**→ **Configuración de iDRAC**→ ficha **Propiedades**→ **Información de acceso remoto**→ **Configuración de red**
- **Sistema**→ **Configuración de iDRAC**→ ficha **Red/Seguridad**→ **Red**→ **Configuración de la tarjeta de interfaz de red**

PRECAUCIÓN: Con la función FlexAddress activada, si se pasa de una dirección MAC asignada por el servidor a una asignada por el chasis y viceversa, la dirección IP del iDRAC6 también cambia.

NOTA: La función FlexAddress sólo puede activarse o desactivarse a través del CMC. La interfaz gráfica de usuario del iDRAC6 sólo muestra el estado. Toda sesión de consola virtual o de medios virtuales finalizará si se modifica la configuración de FlexAddress en la página FlexAddress del CMC.

Activación de FlexAddress a través de RACADM

No se puede activar la función FlexAddress desde el iDRAC6. Active la función FlexAddress en los niveles de red Fabric y ranura del CMC.

1. Desde la consola de CMC, active la función FlexAddress para el servidor administrado en la ranura con el siguiente comando de RACADM:

   `racadm setflexaddr -i <slot_no> 1`, donde `<slot_no>` es el número de ranura en el cual se puede activar la función FlexAddress.

2. Luego, desde la consola de CMC, active la función FlexAddress a nivel de red Fabric ejecutando el siguiente comando de RACADM:

   `racadm setflexaddr -f <fabric_name> 1`, donde `<fabric_name>` es A, B o C.

3. Para activar la función FlexAddress para todos los iDRAC6s en el chasis, desde la consola de CMC, ejecute el siguiente comando de RACADM:

   ```
   racadm setflexaddr -f idrac 1
   ```

Consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) para obtener más información sobre los subcomandos RACADM CMC.

Registro del sistema remoto

La función de registro del sistema remoto del iDRAC6 permite escribir de manera remota el registro del RAC y el registro de sucesos del sistema (SEL) en un servidor de registro del sistema externo. Se pueden leer todos los registros del conjunto completo de servidores desde un registro central.

El protocolo de registro del sistema remoto no necesita ningún tipo de autentificación de usuario. Para introducir los registros en el servidor de registro del sistema remoto, asegúrese de que la conectividad de red entre el iDRAC6 y el servidor de registro del sistema remoto sea correcta y de que el servidor de registro del sistema remoto se ejecute en la misma red que el iDRAC6. Las anotaciones del registro del sistema remoto son paquetes UDP que se envían al puerto de registro del sistema del servidor de registro del sistema remoto. Si se producen errores en la red, el iDRAC6 no vuelve a enviar el mismo registro. El registro remoto ocurre en tiempo real a medida que los registros ingresan al registro SEL y al registro del RAC del iDRAC6. También puede cambiar la configuración de registro del sistema remoto del iDRAC6 a través del CMC.

Para activar Remote Syslog a través de la interfaz de web:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema**→ ficha **Configuración**→ **Configuración del registro del sistema remoto**. Aparece la pantalla **Configuración del registro del sistema remoto**.

La Tabla 2-2 indica la configuración del registro del sistema remoto.

Tabla 2-2. Configuración del registro del sistema remoto

Atributo	Descripción
Registro del sistema remoto activado	Seleccione esta opción para activar la transmisión y captura remota de registro del sistema en el servidor especificado. Una vez activado el registro del sistema, se envían nuevas anotaciones de registro a los servidores de registro del sistema.
Servidor de registro del sistema 1-3	Introduzca la dirección del servidor de registro del sistema remoto para registrar mensajes del iDRAC6 como registros SEL y del RAC. Las direcciones del servidor registro del sistema admiten caracteres alfanuméricos y los símbolos -, ., : y _.
Port Number (Número de puerto)	Introduzca el número de puerto del servidor de registro del sistema remoto. Proporciona un valor entre 1 y 65535. El predeterminado es 514.

NOTA: Los niveles de gravedad que define el protocolo de registro del sistema remoto difieren de los del registro de sucesos del sistema (SEL) de IPMI estándar. En consecuencia, todas las anotaciones de registro del sistema remoto del iDRAC6 se informan al servidor de registro del sistema con niveles de gravedad de **Aviso**.

El siguiente ejemplo muestra los objetos de configuración y el uso del comando de RACADM para cambiar la configuración de registro del sistema remoto:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogEnable [1/0]; default is 0

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer1 <servername1>; default is
blank

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer2 <servername2>; default is
blank
```

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer3 <nombre_del_servidor_3>;
el valor predeterminado es en blanco

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPort <número_de_puerto>; el valor
predeterminado es 514
```

Primer dispositivo de inicio

Esta función permite seleccionar el primer dispositivo de inicio del sistema y activar el inicio único. El sistema se inicia a partir del dispositivo seleccionado en el siguiente reinicio y en los subsiguientes reinicios, y sigue siendo el primer dispositivo de inicio en el orden de inicio del BIOS mientras no sea cambiado nuevamente en la interfaz gráfica de usuario de iDRAC6 o en la secuencia de inicio del BIOS. Si la función Inicio único está activada, el sistema se iniciará una sola vez desde el dispositivo seleccionado. Posteriormente, el sistema se inicia según la secuencia de inicio del BIOS.

Para seleccionar el primer dispositivo de inicio a través de la interfaz web remota:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema**→ ficha **Configurar**→ **Primer dispositivo de inicio**. Aparece la pantalla **Primer dispositivo de inicio**.

La Tabla 2-3 muestra una lista de los valores del **Primer dispositivo de inicio**.

Tabla 2-3. Primer dispositivo de inicio

Atributo	Descripción
Primer dispositivo de inicio	Seleccione el primer dispositivo de inicio en la lista desplegable. El sistema se inicia a partir del dispositivo seleccionado en el reinicio siguiente y en los inicios subsiguientes.
Iniciar una vez	Seleccionado = activado; deseleccionado = desactivado. Seleccione esta opción para iniciar a partir del dispositivo seleccionado en el siguiente inicio. En lo sucesivo, el sistema se inicia a partir del primer dispositivo de inicio en el orden de inicio del BIOS.

Recurso compartido de archivos remotos

La función de uso compartido de archivos remotos a través del iDRAC6 permite especificar un archivo de imagen ISO de CD/DVD ubicado en un recurso compartido de red y ponerlo a disposición del sistema operativo del servidor como unidad virtual montándolo como CD o DVD mediante NFS o CIFS.

NOTA: Esta función sólo funciona con direcciones IPv4. Por el momento, no se admiten direcciones IPv6.

NOTA: En las distribuciones de Linux, esta función puede requerir un comando manual mount cuando funciona a nivel de ejecución init 3.
La sintaxis del comando es:
`mount /dev/OS_specific_device /<user defined mount point>`
donde, `<user defined mount point>` es cualquier directorio que decida utilizar para el montaje similar a cualquier comando mount.
En RHEL, el dispositivo CD (dispositivo virtual **.iso**) es **/dev/scd0** y el disco flexible (dispositivo virtual **.img**) es **/dev/sdc**.
En SLES, el dispositivo CD es **/dev/sr0** y el dispositivo de disco es **/dev/sdc**.
Para asegurarse de que se utiliza el dispositivo correcto (tanto para SLES como para RHEL), al conectar el dispositivo virtual, en el sistema operativo Linux se debe ejecutar inmediatamente el comando:
`tail /var/log/messages | grep SCSI`
Se muestra el texto que identifica al dispositivo (por ejemplo: Dispositivo SCSI sdc), Este procedimiento se aplica a los medios virtuales cuando se utilizan las distribuciones Linux en el nivel de ejecución init 3. En forma predeterminada, los soportes virtuales no se montan automáticamente en init 3.

El formato de la ruta de acceso de la imagen compartida de CIFS es:

```
//<ipaddress or domain
name>/<share_name>/<pathtoimage>
```

El formato de la ruta de acceso de la imagen compartida de NFS es:

```
<ipadddress>:/<pathtoimage>
```

Si el nombre de usuario incluye un nombre de dominio, se debe introducir el nombre de usuario de la siguiente manera *<user name>@<domain>*. Por ejemplo, **user1@dell.com** es un nombre de usuario válido, mientras que **dell\user1** no lo es.

El nombre de archivo que termine con la extensión IMG es redireccionado como disco flexible virtual y el nombre de archivo que termine con la extensión ISO es redireccionado como CDROM virtual. El recurso compartido de archivos remotos admite sólo formatos de archivo de imagen .IMG e .ISO.

La función RFS utiliza la implementación de soportes virtuales subyacentes en iDRAC6. Debe tener privilegios de medios virtuales para realizar un montaje de RFS. Si medios virtuales ya utiliza una unidad virtual, la unidad no estará disponible para montar un RFS y viceversa. Para que RFS funcione, los medios virtuales del iDRAC6 deben estar configurados en los modos *Conectar* o *Conectar automáticamente*.

El estado de conexión del RFS se encuentra en el registro del iDRAC6. Una vez conectado, el RFS montado en la unidad virtual no se desconecta, incluso si se cierra la sesión del iDRAC6. La conexión del RFS se cierra si se restablece el iDRAC6 o se pierde la conexión a la red. Las opciones interfaz gráfica del usuario y línea de comandos también se encuentran disponibles en CMC e iDRAC6 para cerrar la conexión del RFS. La conexión del RFS desde el CMC siempre anula el montaje de RFS existente en iDRAC6.

NOTA: La función vFlash del iDRAC6 y el RFS no están relacionados.

Para activar la función de archivos remotos compartidos a través de la interfaz web de iDRAC6, haga lo siguiente:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Seleccione **Sistema**→ ficha **Uso compartido de archivos remotos**.

   Aparece la pantalla **Recursos compartidos de archivos remotos**.

La Tabla 2-4 indica la configuración de los recursos compartidos de archivos remotos.

Tabla 2-4. Configuración del servidor de archivos remotos

Atributo	Descripción
Nombre de usuario	Nombre de usuario para conectarse al sistema de archivos NFS/CIFS.
Contraseña	Contraseña para conectarse al sistema de archivos NFS/CIFS.

Tabla 2-4. Configuración del servidor de archivos remotos *(continuación)*

Atributo	Descripción
Ruta de acceso del archivo de imagen	Ruta de acceso del archivo a compartir a través de recursos compartidos de archivos remotos.
Estado	**Conectado**: el archivo se comparte. **No conectado**: el archivo no se comparte. **Conectando...**: ocupado mientras se conecta al recurso compartido.

4 Haga clic en **Conectar** para establecer una conexión de uso compartido de archivos. El botón **Conectar** se desactiva una vez establecida la conexión.

NOTA: Incluso si ha configurado la función recursos compartidos de archivos remotos, la interfaz gráfica de usuario no muestra esta información por razones de seguridad.

Para el uso compartido de archivos remotos, el comando de RACADM remoto es

`racadm remoteimage`.

`racadm remoteimage <options>`

Las opciones son:

`-c`: conectar imagen

`-d`: desconectar imagen

`-u` <username>; nombre de usuario para acceder al recurso compartido de red

`-p` <password>; contraseña para acceder al recurso compartido de red

`-l` <image_location>; ubicación de la imagen en el recurso compartido de red; indique la ubicación entre comillas dobles

`-s`: mostrar el estado actual

PRECAUCIÓN: Todos los caracteres, incluidos los especiales y alfanuméricos, están permitidos para nombre_de_usuario, contraseña y ubicación_de_imagen excepto los siguientes caracteres: ' (apóstrofo), " (comillas), , (comas), < (signo de menor) y > (signo de mayor). Al recurrir al uso compartido de archivos remotos, los caracteres anteriormente indicados no se permiten para el nombre de usuario, la contraseña ni la ubicación de la imagen.

Módulo SD dual interno

El módulo SD dual interno (IDSDM) sólo está disponible en determinadas plataformas. IDSDM proporciona redundancia en la tarjeta SD hipervisor utilizando otra tarjeta SD que refleja el contenido de la primera tarjeta SD. La tarjeta vFlash SD del iDRAC6, con la segunda tarjeta SD, puede configurarse como IDSDM definiendo la opción **Redundancia** en **Modo reflejado** en la pantalla **Dispositivos integrados** de la configuración del BIOS del sistema. Si la función IDSDM está activada, la funcionalidad vFlash de la tarjeta vFlash SD del iDRAC6 no está disponible y esta tarjeta está configurada como la tarjeta SD secundaria del IDSDM. Para obtener más información acerca de las opciones del BIOS para IDSDM, consulte el *Manual del propietario del hardware*, disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

NOTA: En la configuración del BIOS, en la pantalla **Dispositivos integrados**, la opción **Puerto USB interno** debe estar establecida en **Encendido**. Si se configura en **Apagado**, el IDSDM no será visible para el sistema como dispositivo de inicio.

Cualquiera de las dos tarjetas SD puede ser la maestra. Por ejemplo, si se instalan dos tarjetas SD nuevas en el IDSDM, la tarjeta SD1 se convertirá en la tarjeta activa o maestra. La SD2 será la tarjeta en espera y todas las escrituras IDSDM del sistema de archivos irán a ambas tarjetas, pero sólo se realizarán lecturas de la SD1. En cualquier momento que la SD1 falle o se extraiga, la SD2 automáticamente se convertirá en la tarjeta (maestra) activa.

Tabla 2-5. Estado del IDSDM

IDSDM: Modo de reflejo	Tarjeta SD	Tarjeta vFlash SD
Enabled	Activa (Tarjeta SD1)	vFlash inactiva, SD2 en espera
Disabled	Activa (tarjeta SD2)	Sólo vFlash activa

Utilizando el iDRAC, se puede ver el estado, la condición y la disponibilidad del IDSDM.

El estado de redundancia de la tarjeta SD y los sucesos de falla se registran en SEL, se muestran en LCD, y se generan alertas PET si las alertas están activadas.

Visualización del estado del módulo de SD doble interno mediante la interfaz gráfica de usuario

1. Inicie sesión en la interfaz gráfica del usuario de web del iDRAC.
2. En el árbol del **sistema**, haga clic en **Medios Flash extraíbles**. Aparece la página **Medios vFlash extraíbles**. En esta página se muestran las dos secciones siguientes:

- **Módulo SD dual interno**: se muestra sólo si IDSDM está en modo redundante. El **Estado de redundancia** aparece como **Total**. Si esta sección no está presente, la tarjeta está en el estado de modo no redundante. Las indicaciones para el **Estado de redundancia** válida, son:
  - **Total**: las tarjetas SD 1 y 2 funcionan correctamente.
  - **Perdido**: una o ambas tarjetas SD no funcionan correctamente.
- **Estado del módulo SD interno**: muestra el estado de la tarjeta SD en SD1 y SD2 con la información siguiente:
  - Estado:
    - : indica que la tarjeta está bien.
    - : indica que la tarjeta está fuera de línea o protegida contra escritura.
    - : indica que se ha emitido una alerta.
  - Ubicación: ubicación de las tarjetas SD.
  - Estado en línea: las tarjetas SD1 y SD2 pueden estar en uno de los estados indicados en Tabla 2-6.

Tabla 2-6. Estados de las tarjetas SD1 y SD2

State (Estado)	Descripción
Boot (Inicio)	El controlador se está encendiendo.
Activo	La tarjeta recibe todas las escrituras SD y se utiliza para lecturas SD.
En espera	La tarjeta es la tarjeta secundaria. Está recibiendo una copia de todas las escrituras SD.
Ha fallado	Se registró un error durante una operación de lectura o escritura de tarjeta SD.

Tabla 2-6. Estados de las tarjetas SD1 y SD2 ***(continuación)***

State (Estado)	Descripción
Ausente	No se detectó la tarjeta SD
Fuera de línea	Durante el inicio, la firma CID de la tarjeta es diferente del valor de almacenamiento NV o la tarjeta es el destino de una operación de copia que está en curso.
Protegida contra escritura	La tarjeta está protegida contra escritura por el pestillo de la tarjeta SD. El IDSDM no puede utilizar una tarjeta protegida contra escritura.

Actualización del firmware de iDRAC6

La actualización del firmware del iDRAC6 instala una nueva imagen del firmware en la memoria flash. Puede actualizar el firmware por alguno de los métodos siguientes:

- Interfaz web del iDRAC6
- CLI de RACADM
- Dell Update Package (para Linux o Microsoft Windows)
- La utilidad de actualización del firmware del iDRAC6 de DOS
- Interfaz web del CMC
- Interfaz WSMAN

Descarga del firmware o el paquete de actualización

Descargue el firmware en **support.dell.com**. La imagen del firmware está disponible en varios formatos a fin de admitir los distintos métodos de actualización disponibles.

Para actualizar el firmware del iDRAC6 por medio de la interfaz web del iDRAC6 o para recuperar el iDRAC6 mediante la interfaz web del CMC, descargue la imagen binaria que viene comprimida como archivo de extracción automática.

Para actualizar el firmware del iDRAC6 desde el servidor administrado, descargue el Dell Update Package (DUP) para el sistema operativo que se ejecuta en el servidor cuyo iDRAC6 va a actualizar.

Para actualizar el firmware del iDRAC6 por medio de la utilidad de actualización del firmware del iDRAC6 de DOS, descargue la utilidad de actualización y la imagen binaria, que vienen comprimidas en archivos de extracción automática.

Ejecutar la actualización del firmware

NOTA: Cuando la actualización de firmware del iDRAC6 comienza, todas las sesiones existentes en el iDRAC6 se desconectan y no se permiten nuevas sesiones hasta que el proceso de actualización haya terminado.

NOTA: Los ventiladores del chasis funcionan al 100 % durante la actualización de firmware del iDRAC6. Cuando la actualización concluya, se reanudará la regulación normal de la velocidad de los ventiladores. Éste es el comportamiento normal y fue diseñado para proteger el servidor contra sobrecalentamientos durante el periodo en que no se puede enviar información del sensor al CMC.

Para utilizar un Dell Update Package para Linux o Microsoft Windows, ejecute el DUP específico para el sistema operativo en el servidor administrado.

Cuando utiliza la interfaz web del iDRAC6 o la interfaz web del CMC, coloque la imagen binaria del firmware en un disco al que se pueda acceder desde la estación de administración en la que usted ejecuta la interfaz web. Vea la "Actualización del firmware de iDRAC6" en la página 129.

NOTA: La interfaz web del iDRAC6 también permite restablecer la configuración predeterminada de fábrica del iDRAC6.

NOTA: Si no se conserva la configuración durante la actualización del firmware, el iDRAC6 genera nuevas claves SHA1 y MD5 para el certificado SSL. Como las claves son diferentes a las del explorador web abierto, todas las ventanas del explorador que están conectadas al iDRAC6 deben cerrarse después de finalizar la actualización del firmware. Si las ventanas del explorador no se cierran, se verá el mensaje de error **Certificado no válido.**

Puede utilizar la interfaz web del CMC o RACADM del CMC para actualizar el firmware del iDRAC6. Esta función está disponible cuando el firmware del iDRAC6 está en modo Normal y cuando está dañado. Vea la "Actualización del firmware del iDRAC6 por medio del CMC" en la página 131.

NOTA: Si está realizando una reversión del firmware del iDRAC6 a una versión anterior, elimine el complemento ActiveX del explorador Internet Explorer de cualquier estación de administración basada en Windows para permitir que el firmware instale una versión compatible del complemento ActiveX.

Verificación de la firma digital para los DUP de Linux

La firma digital se utiliza para autentificar la identidad del firmante de un archivo y para certificar que el contenido original del archivo no se ha modificado desde que se firmó.

Si aún no lo tiene instalado en el sistema, deberá instalar el Resguardo de privacidad GNU (GPG, por sus siglas en inglés) para verificar firmas digitales.

Para utilizar el procedimiento estándar de verificación, realice los pasos siguientes:

1. Descargue la clave GnuPG pública de Linux de Dell de la siguiente manera: Visite **lists.us.dell.com** y haga clic en el vínculo **Clave GPG pública de Dell**. Guarde el archivo en el sistema local. El nombre predeterminado es **linux-security- publickey.txt**.
2. Para importar la clave pública a la base de datos de confianza de GPG, ejecute el siguiente comando:

   gpg --import <Public Key Filename>
3. Para evitar un aviso de clave no confiable, cambie el nivel de confianza de la clave GPG pública de Dell.
   a. Introduzca el comando siguiente:

      `gpg --edit-key 23B66A9D`

   b. Dentro del editor de claves GPG, introduzca `fpr`. Aparece el mensaje siguiente:

      ```
      pub 1024D/23B66A9D 2001-04-16 Dell, Inc.
      (Product Group) <linux-security@dell.com>
      Primary key fingerprint: 4172 E2CE 955A 1776
      A5E6 1BB7 CA77 951D 23B6 6A9D
      ```

      Si la huella digital de la clave importada es igual a la anterior, usted tiene una copia correcta de la clave.

   c. Mientras aún está en el editor de claves GPG, introduzca `trust`. Aparece el mensaje siguiente:

      ```
      Decida el nivel de confianza que otorga a este
      usuario a fin de verificar correctamente las
      claves de otros usuarios (revisando pasaportes,
      ```

```
comprobando huellas digitales de distintas
fuentes, etc.)

  1 = no sé o me abstengo
  2 = no confío en él
  3 = confío en él con reservas
  4 = confío en él
  5 = confío en él plenamente
  m = regresar al menú principal

¿Cuál es su decisión?
```

d Introduzca `5` y luego presione <Intro>. Aparece el mensaje siguiente:

```
¿Realmente desea otorgar plena confianza a esta
clave? [y/N]
```

e Introduzca `y` <Intro> para confirmar su elección.

f Introduzca `quit` <Intro> para salir del editor de claves GPG.

Debe importar y validar la clave pública sólo una vez.

4 Obtenga el paquete que necesita (por ejemplo, el DUP de Linux o el archivo de extracción automática) y el archivo de firma asociado del sitio web del servicio de asistencia Dell Support en **support.dell.com/support/downloads**.

NOTA: Cada paquete de actualización de Linux tiene un archivo de firma independiente, que aparece en la misma página web que el paquete de actualización. Se necesita el paquete de actualización y el archivo de firma relacionado para la verificación. De manera predeterminada, el archivo de firma tiene el mismo nombre que el archivo DUP con la extensión **.sign**. Por ejemplo, la imagen del firmware del iDRAC6 tiene un archivo **.sign** asociado (**IDRAC_FRMW_LX_2.2.BIN.sign**) que se incluye en el archivo de extracción automática con la imagen del firmware (**IDRAC_FRMW_LX_2.2.BIN**). Para descargar los archivos, haga clic con el botón derecho del mouse en el vínculo de **descarga** y utilice la opción **Guardar destino como...**

5 Verifique el paquete de actualización:

```
gpg --verify <nombre del archivo de firma del
paquete de actualización de Linux> <nombre de
archivo del paquete de actualización de Linux>
```

El ejemplo siguiente ilustra los pasos a seguir para verificar un paquete de actualización de Dell PowerEdge M610 iDRAC6:

1. Descargue los dos archivos siguientes en **support.dell.com**:
   - IDRAC_FRMW_LX_2.2.BIN.sign
   - IDRAC_FRMW_LX_2.2.BIN
2. Importe la clave pública mediante la ejecución de la siguiente línea de comandos:

   ```
   gpg --import <linux-security-publickey.txt>
   ```

   Aparece el mensaje de salida siguiente:

   ```
   gpg: clave 23B66A9D: "Dell Computer Corporation
   (Linux Systems Group) <linux-
   security@dell.com>" no se modificó
   gpg: Número total procesado: 1
   gpg: Sin modificar: 1
   ```

3. Establezca el nivel de confianza de GPG para la clave pública de Dell, si aún no lo ha hecho.
   a. Introduzca el comando siguiente:

      ```
      gpg --edit-key 23B66A9D
      ```

   b. En el símbolo del sistema, introduzca los comandos siguientes:

      ```
      fpr
      trust
      ```

   c. Introduzca `5` y luego presione <Intro> para elegir `confío plenamente` en el menú.
   d. Introduzca `y` <Intro> para confirmar su elección.
   e. Introduzca `quit` <Intro> para salir del editor de claves GPG.

   Esto completa la validación de la clave pública de Dell.
4. Verifique la firma digital del paquete Dell PowerEdge M610 del iDRAC6 mediante la ejecución del comando siguiente:

   ```
   gpg --verify IDRAC_FRMW_LX_2.2.BIN.sign
   IDRAC_FRMW_LX_2.2.BIN
   ```

Aparece el mensaje de salida siguiente:

```
gpg: Firma realizada Vie Jul 11 15:03:47 2008
CDT utilizando clave DSA ID 23B66A9D
gpg: Buena firma de "Dell, Inc. (grupo del
producto) <linux-security@dell.com>"
```

Si no ha validado la clave como se muestra en el paso 3, recibirá mensajes adicionales:

```
gpg: AVISO: Esta clave no está certificada con una
firma confiable.
gpg: No hay indicación de que la firma pertenezca al
propietario.
Huella digital de clave primaria: 4172 E2CE 955A 1776
A5E6 1BB7 CA77 951D 23B6 6A9D
```

Uso de la interfaz web del iDRAC6

NOTA: Si se interrumpe el progreso de la actualización del firmware del iDRAC6 antes de que se complete, el firmware del iDRAC6 podría dañarse. En tal caso, puede recuperar el iDRAC6 desde la interfaz web del CMC.

NOTA: De manera predeterminada, la actualización del firmware conserva la configuración actual del iDRAC6. Durante el proceso de actualización, tiene la opción de restablecer la configuración predeterminada de fábrica del iDRAC6. Si establece la configuración predeterminada de fábrica, el acceso a la red externa se desactivará cuando la actualización termine. Debe activar y configurar la red por medio de la utilidad de configuración del iDRAC6.

1. Inicie la interfaz web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC**.
3. Haga clic en la ficha **Actualizar**.

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

   NOTA: Para actualizar el firmware, el iDRAC6 debe estar en el modo de actualización. Cuando se encuentre en este modo, el iDRAC6 se restablecerá automáticamente, aun cuando usted cancele el proceso de actualización.
4. En la sección **Cargar**, haga clic en **Examinar** para ubicar la imagen del firmware que descargó. El nombre predeterminado de la imagen del firmware es **firmimg.imc**.

5 Haga clic en **Cargar**.

El archivo se cargará en el iDRAC6. This may take several minutes to complete.

NOTA: Durante el proceso de carga, puede anular el proceso de actualización del firmware al hacer clic en **Cancelar**. Al hacer clic en **Cancelar,** el iDRAC6 se restablecerá al modo de operación normal.

Una vez que la carga ha finalizado, aparece la pantalla **Cargar (paso 2 de 3)**.

- Si el archivo de imagen se carga satisfactoriamente y pasa todas las revisiones de verificación, aparecerá un mensaje indicando que la imagen del firmware ha sido verificada.
- Cuando la imagen no se cargue correctamente o cuando no pase las revisiones de verificación, la actualización del firmware regresará a la pantalla **Actualización del firmware**. Puede intentar actualizar el iDRAC6 nuevamente o hacer clic en **Cancelar** para restablecer el iDRAC6 al modo de operación normal.

NOTA: Si deselecciona la casilla de verificación **Conservar configuración**, el iDRAC6 restablecerá la configuración predeterminada. En la configuración predeterminada, la LAN está desactivada y no se puede iniciar sesión en la interfaz web del iDRAC6. Debe reconfigurar los valores de la LAN por medio de la **utilidad de configuración del iDRAC6** durante la POST del BIOS o a través del CMC.

6 De manera predeterminada, la casilla de verificación **Conservar configuración** está activada (seleccionada) para conservar los valores actuales en el iDRAC6 después de una actualización. Si no desea conservar los valores, deseleccione la casilla de verificación de marcación **Conservar configuración**.

7 Haga clic en **Comenzar la actualización** para iniciar el proceso de actualización. No interrumpa el proceso de actualización.

8 En la página **Cargar (paso 3 de 3)**, verá el estado de la carga. El progreso de la operación de actualización de firmware, expresado en porcentaje, aparece en la columna **Progreso**.

9 Una vez finalizada la actualización de firmware, la ventana **Cargar (paso 3 de 3)** se actualiza con el resultado y el iDRAC6 se restablece automáticamente. Debe cerrar la ventana actual del explorador y volver a conectarse al iDRAC6 desde una ventana nueva de explorador.

Actualización del firmware del iDRAC6 por medio de RACADM

Puede actualizar el firmware del iDRAC6 mediante RACADM remoto.

1. Puede descargar la imagen del firmware del iDRAC6 a través del sitio web del servicio de asistencia Dell Support en **support.dell.com** en el servidor TFTP.

   Por ejemplo,

   C:\downloads\firmimg.imc

2. Ejecute el siguiente comando de RACADM:

   Por ejemplo,

   ```
   racadm -r <iDRAC6 IP address> -u <username> -p
   <password> fwupdate -g -u -a <path>
   ```

   donde *ruta de acceso* es la ubicación en el servidor TFTP en la que está almacenado **firmimg.imc**.

Uso de la utilidad de actualización de DOS

Para actualizar el firmware del iDRAC6 por medio de la utilidad de actualización de DOS, inicie el servidor administrado en DOS y ejecute el comando **idrac16d**. La sintaxis del comando es:

```
idrac16d [-f] [-i=<filename>] [-l=<logfile>]
```

Cuando se ejecuta sin agregar opciones, el comando **idrac16d** actualiza el firmware del iDRAC6 con el archivo de imagen de firmware **firmimg.imc** en el directorio actual.

Las opciones son las siguientes:

- `-f`: fuerza la actualización. La opción `-f` se puede utilizar para *degradar* el firmware a una imagen anterior.
- `-i=<nombre de archivo>`: Especifica el nombre del archivo que contiene la imagen de firmware. Esta opción es necesaria cuando el nombre de archivo predeterminado del firmware, **firmimg.imc**, ha sido cambiado.
- `-l=<archivo_de_registro>`: Registra la salida de la actividad de actualización. Esta opción se utiliza para depuración.

NOTA: Si usted introduce argumentos incorrectamente con el comando **idrac16d** o añade la opción `-h`, tal vez note la opción adicional `-nopresconfig` en el mensaje de salida sobre el uso. Esta opción se usa para actualizar el firmware sin conservar la información de configuración. Se recomienda **no** utilizar esta opción ya que *elimina* toda su información de configuración del iDRAC6, como direcciones IP, usuarios y contraseñas.

Uso de la interfaz WSMAN

Para obtener más información sobre cómo actualizar el firmware utilizando WSMAN, consulte la documentación disponible en el Enterprise Technology Center de Dell en **delltechcenter.com**.

Actualización del paquete de reparación de USC

Consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller) para obtener más información acerca de la actualización del paquete de reparación de USC desde la interfaz web del iDRAC6.

Configuración del iDRAC6 para utilizarlo con IT Assistant

Dell OpenManage IT Assistant puede descubrir dispositivos administrados que cumplan con las versiones 1 y 2c del protocolo simple de administración de red (SNMP) y la versión 2.0 de la interfaz de administración de plataforma inteligente (IPMI).

El iDRAC6 cumple con IPMI versión 2.0. En esta sección se describen los pasos necesarios para configurar el iDRAC6 para descubrimiento y supervisión a través de IT Assistant. Existen dos formas de llevar a cabo este procedimiento: Mediante la utilidad de configuración del iDRAC6 y por medio de la interfaz gráfica web del iDRAC6.

Uso de la utilidad de configuración del iDRAC6 para activar las funciones de descubrimiento y supervisión

Para configurar el iDRAC6 para el descubrimiento de IPMI y el envío de capturas de alerta por medio de la utilidad de configuración del iDRAC6, reinicie el servidor administrado (blade) y controle el proceso de encendido por medio de la consola virtual y un teclado de consola y supervisión remota o bien una comunicación en serie en la LAN (SOL). Cuando aparezca la indicación `Presione <Ctrl-E> for Remote Access Setup`, presione <Ctrl><E>.

Cuando aparezca la pantalla **Utilidad de configuración** del iDRAC6, utilice las teclas de flechas para desplazarse hacia abajo.

1. Activar **IPMI en la LAN**
2. Introduzca la **Clave de cifrado RMCP+** del sitio, si utiliza una.

   NOTA: Consulte al administrador de red o al director de IT para analizar la posibilidad de implementar esta opción, ya que agrega una valiosa protección de la seguridad y debe implementarse en todo el sitio para que funcione correctamente.
3. En la sección **Parámetros de LAN**, presione <Intro> para entrar a la pantalla secundaria. Utilice las teclas de flecha hacia arriba y hacia abajo para recorrer la pantalla.
4. Con la barra espaciadora, **active** la opción **Alerta de LAN activada**.
5. Introduzca la dirección IP de su estación de administración en **Destino de alerta 1**.
6. En **Nombre de iDRAC6**, introduzca un nombre que cumpla con la convención utilizada en el centro de datos. El nombre predeterminado es `iDRAC6-{`*`Etiqueta de servicio`*`}`.

Para salir de la utilidad de configuración del iDRAC6 presione <Esc>, <Esc> y luego <Intro> para guardar los cambios. El servidor se iniciará en el modo de operación normal e IT Assistant lo detectará durante la próxima pasada de descubrimiento programada.

NOTA: También puede utilizar la consola de administración Dell, la aplicación de administración de uno a varios sistemas de próxima generación, para activar el descubrimiento y la supervisión. Para obtener más información, consulte la *Dell Management Console User's Guide* (Guía del usuario de Dell Management Console) en el sitio web de asistencia de Dell, en **dell.com/support/manuals**.

Uso de la interfaz web del iDRAC6 para activar las funciones de descubrimiento y supervisión

El descubrimiento de IPMI también puede activarse a través de la interfaz web remota:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6 con el nombre de usuario y la contraseña con derechos de administrador.
3. En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC→** ficha **Red/Seguridad.**

   Se muestra la pantalla **Red.**
4. En la sección **Configuración de IPMI**, asegúrese de que la casiila **Activar IPMI sobre LAN** está seleccionada (verificado).
5. Seleccione **Administrador** en el menú desplegable **Límite de nivel de privilegio del canal**.
6. Introduzca la **Clave de cifrado RMCP+** del sitio, si utiliza una.
7. Haga clic en **Aplicar** si realizó cambios en esta pantalla.
8. En el árbol del sistema, seleccione **Sistema→** ficha **Administración de alertas→ Sucesos de plataforma**.

   Aparecerá la pantalla **Sucesos de plataforma** con una lista de sucesos para los cuales puede configurar iDRAC6 para generar alertas por correo electrónico.
9. Active las alertas por correo electrónico para uno o más sucesos seleccionando la casilla de verificación en la columna **Generar alertas**.
10. Haga clic en **Aplicar** si realizó cambios en esta pantalla.
11. Haga clic en **Valores de captura**. Aparecerá la pantalla **Valores de captura.**
12. En la sección **Lista de destinos de IPv4**, en el primer campo disponible **Dirección IP de destino**, seleccione la casilla de verificación **Activada** y, a continuación, la dirección IP de su Management Station.
13. Repita el paso 12 para la sección **Lista de destino IPv6**.
14. Haga clic en **Aplicar**. Puede hacer clic en **Enviar** para enviar una alerta de captura de prueba.

15 Haga clic en **Configuración de alertas de correo electrónico**. Se muestra la pantalla **Configuración de alertas de correo electrónico**.

16 En la sección **Direcciones de correo electrónico de destino**, en el primer campo disponible **Alerta por correo electrónico**, escriba la dirección de correo electrónico que deben recibir los mensajes de alerta; a continuación, haga clic en **Aplicar**.

17 Puede hacer clic en **Enviar** para enviar una alerta de captura de prueba.

Por motivos de seguridad, Dell recomienda especialmente crear un usuario aparte para los comandos de IPMI con un nombre de usuario, privilegios de IPMI en la LAN y contraseña propios:

1 En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC**.

2 Haga clic en la ficha **Red/Seguridad** y luego en **Usuarios**.

Aparecerá la pantalla **Usuarios** con una lista de todos los usuarios (definidos o no definidos).

3 Haga clic en la **Identificación de usuario** de un usuario no definido.

Aparecerá la pantalla **Configuración de usuario** para la identificación de usuario que seleccionó.

4 Seleccione la casilla de verificación **Activar usuario** y luego introduzca el nombre de usuario y la contraseña.

5 En la sección **Privilegios de LAN de IPMI**, asegúrese de que **Privilegio máximo permitido de usuario de LAN** esté definido como **Administrador**.

6 Establezca los privilegios de usuario.

7 Haga clic en **Aplicar** para guardar la configuración de nuevos usuarios.

Uso de IT Assistant para ver el estado y los sucesos del iDRAC6

Después de completar el descubrimiento, los dispositivos iDRAC6 aparecerán en la categoría **Servidores** de la pantalla **Detalles de dispositivos ITA** y la información del iDRAC5 podrá visualizarse al hacer clic en el nombre del iDRAC6. Esto difiere de los sistemas DRAC 5, en los que la tarjeta de administración aparece en el grupo de RAC.

Las capturas de avisos y errores de iDRAC6 ahora pueden visualizarse en el **Registro de alertas** principal de IT Assistant. Aunque aparecen en la categoría **Desconocido**, la descripción y gravedad de las capturas se indican con exactitud.

Para obtener más información acerca del uso de IT Assistant para administrar el centro de datos, consulte la *Dell OpenManage IT Assistant User's Guide* (Guía del usuario de Dell OpenManage IT Assistant).

NOTA: También puede utilizar la consola de administración Dell, la aplicación de administración de uno a varios sistemas de próxima generación, para ver los sucesos y el estado del iDRAC6. Para obtener más información, consulte la *Dell Management Console User's Guide* (Guía del usuario de Dell Management Console) en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

3

Configuración de la estación de administración

Una estación de administración es un equipo que se usa para supervisar y administrar los servidores Dell PowerEdge y otros módulos en el chasis. Esta sección describe la instalación del software y las tareas de configuración que preparan una estación de administración para trabajar con iDRAC6 Enterprise. Antes de comenzar a configurar el iDRAC6, siga los procedimientos de esta sección para asegurarse de haber instalado y configurado las herramientas que necesitará.

Pasos de configuración de la estación de administración

Para configurar estación de administración, realice los pasos a continuación:

1. Configure la red de la estación de administración.
2. Instale y configure un explorador web admitido.
3. Instale Java Runtime Environment (JRE) (requisito si utiliza el tipo de complemento de Java).
4. Instale clientes SSH o Telnet, de ser necesario.
5. Instale a un servidor TFTP, de ser necesario.
6. Instale Dell OpenManage IT Assistant (opcional).
7. Instale la consola de administración Dell (opcional).

Requisitos de la red de la estación de administración

Para tener acceso al iDRAC6, la estación de administración debe estar en la misma red que el puerto de conexión RJ45 del CMC que está etiquetado como "GB1". Es posible aislar la red del CMC de la red en la que se encuentra el servidor administrado, de modo que la estación de administración pueda tener acceso por LAN al iDRAC6 pero no al servidor administrado.

Por medio de la función de consola virtual del iDRAC6 (ver "Configuración y uso de la comunicación en serie en la LAN" en la página 207), es posible acceder a la consola del servidor administrado aun sin acceso de red a los puertos del servidor. Usted también puede ejecutar diversas funciones de administración en el servidor administrado, como por ejemplo reiniciar el equipo y usar los servicios del iDRAC6. Sin embargo, para tener acceso a la red y a los servicios de aplicación que se encuentran en el servidor administrado, es posible que necesite tener un NIC adicional en el servidor administrado.

Configuración de un explorador web admitido

Las secciones siguientes contienen instrucciones para configurar los exploradores web admitidos para usar con la interfaz web del iDRAC6.

Abrir el explorador web

La interfaz web del iDRAC6 está diseñada para verse en un explorador web admitido con una resolución de pantalla mínima de 800 píxeles de ancho por 600 de alto. Para visualizar la interfaz y acceder a todas las funciones, asegúrese de que la resolución esté configurada al menos en 800 por 600 píxeles y/o cambie el tamaño del explorador, según sea necesario.

NOTA: En algunas situaciones, con frecuencia durante la primera sesión después de una actualización del firmware, los usuarios de Internet Explorer verán el mensaje **Listo, pero con errores** en la barra de estado del explorador junto con una pantalla parcialmente procesada en la ventana principal. Este error también puede ocurrir si está experimentando problemas de conectividad. Éste es un problema conocido con Internet Explorer. Cierre el explorador y vuelva a comenzar.

Configuración del explorador web para conectarse a la interfaz web

Si se conecta a la interfaz web del iDRAC6 desde una estación de administración que se conecta a Internet mediante un servidor proxy, debe configurar el explorador web para que acceda a Internet desde este servidor.

Para configurar el explorador web Internet Explorer para acceder a un servidor proxy, realice los pasos a continuación:

1. Abra una ventana del explorador web.
2. Haga clic en **Herramientas** y en **Opciones de Internet**.

   Se muestra la ventana **Opciones de internet**.

3 Seleccione **Herramientas→ Opciones de Internet→ Seguridad→ Red local**.

4 Haga clic en **Nivel personalizado**.

5 Seleccione la opción **Medio bajo** en el menú desplegable y luego haga clic en **Restablecer**. Haga clic en **Aceptar** para confirmar. Deberá hacer clic en este botón para regresar al cuadro de diálogo **Nivel personalizado**.

6 Desplácese hacia abajo hasta la sección de controles y complementos de ActiveX y verifique cada configuración, pues las distintas versiones de IE muestran diferentes valores para el estado **Medio bajo**:

- Preguntar automáticamente si se debe usar un control ActiveX: activar
- Comportamiento de binarios y de secuencias de comandos: activar
- Descargar los controles ActiveX firmados: Preguntar
- Inicializar y generar secuencias de comandos de los controles ActiveX no marcados como seguros: Preguntar
- Ejecutar controles y complementos de ActiveX: activar
- Generar secuencias de comandos de los controles ActiveX marcados como seguros para Secuencias de comandos: activar

En la sección de **Descargas**:

- Preguntar automáticamente si se debe descargar un archivo: activar
- Descarga de archivos: activar
- Descarga de fuentes: activar

En la sección **Miscelánea**:

- Permitir META-REFRESH: activar
- Permitir la ejecución de secuencias de comandos en el control del explorador web de Internet Explorer: activar
- Permitir que se abran ventanas generadas por secuencias de comandos sin restricción de tamaño ni posición: activar
- No pedir que se seleccione un certificado de cliente cuando exista sólo uno o cuando no exista ninguno: activar
- Ejecutar programas y archivos en IFRAME: activar
- Abrir archivos basándose en el contenido, no en la extensión de archivo: activar

- Permisos de canal de software: Seguridad baja
- Enviar los datos no cifrados del formulario: activar
- Usar el bloqueador de elementos emergentes: Desactivar

En la sección **Automatización**:

- Secuencia de comandos activa: activar
- Permitir operaciones de pegado por medio de una secuencia de comandos: activar
- Secuencias de comandos de applets de Java: activar

7 Seleccione **Herramientas→ Opciones de Internet→ Opciones avanzadas**.

8 Verifique que las siguientes opciones se encuentren seleccionadas o deseleccionadas, según corresponda:

En la sección **Examinar**:

- Enviar direcciones URL en UTF-8: Seleccionada
- Desactivar la depuración de secuencias de comandos (Internet Explorer): Seleccionada
- Desactivar la depuración de secuencias de comandos (otros): Seleccionada
- Mostrar una notificación sobre cada error de secuencia de comandos: Deseleccionada
- Activar la instalación a petición (otros): Seleccionada
- Activar transiciones de página: Seleccionada
- Activar extensiones de explorador de terceros: Seleccionada
- Iniciar accesos directos en ventanas ya abiertas: Deseleccionada

En la sección **Configuración de HTTP 1.1**:

- Usar HTTP 1.1: Seleccionada
- Usar HTTP 1.1 en conexiones proxy: Seleccionada

En la sección **Java (Sun)**:

- Utilizar JRE 1.6.x_yz: Seleccionada (opcional; la versión puede diferir)

En la sección **Multimedia**:

- Activar Cambio automático del tamaño de imágenes: Seleccionada

- Activar animaciones en páginas web: Seleccionada
- Mostrar videos en páginas web: Seleccionada
- Mostrar imágenes: Seleccionada

En la sección **Seguridad**:

- Comprobar si se revocó el certificado del editor: Deseleccionada
- Comprobar si existen firmas en los programas descargados: Deseleccionada
- Comprobar si existen firmas en los programas descargados: Seleccionada
- Usar SSL 2.0: Deseleccionada
- Usar SSL 3.0: Seleccionada
- Usar TLS 1.0: Seleccionada
- Advertir sobre certificados de sitios no válidos: Seleccionada
- Advertir si se cambia entre un modo seguro y un modo no seguro: Seleccionada
- Advertir si se redirige el envío de formularios: Seleccionada

NOTA: Si decide cambiar alguna de las opciones anteriores, se recomienda aprender y comprender correctamente las consecuencias de cada acción. Por ejemplo, si opta por bloquear los mensajes emergentes, ciertas partes de la interfaz web del iDRAC6 no funcionarán correctamente.

9 Haga clic en **Aplicar** y después en **Aceptar**.

10 Haga clic en la ficha **Conexiones**.

11 En **Configuración de la red de área local (LAN)**, haga clic en **Configuración de LAN**.

12 Si la casilla **Usar servidor proxy** está seleccionada, seleccione la casilla **No usar servidor proxy para direcciones locales**.

13 Haga clic dos veces en **Aceptar**.

14 Cierre y reinicie el explorador para asegurarse de que todos los cambios tengan efecto.

Cómo agregar el iDRAC6 a la lista de dominios de confianza

Al acceder a la interfaz web del iDRAC6 a través del explorador web, es posible que se le pida que agregue la dirección IP del iDRAC6 a la lista de dominios de confianza si dicha dirección IP no figura en la lista. Al terminar, haga clic en **Actualizar** o vuelva a iniciar el explorador web para establecer una conexión con la interfaz web del iDRAC6.

Es posible que en algunos sistemas operativos, Internet Explorer (IE) 8 no le solicite que agregue la dirección IP de iDRAC6 a la lista de los dominios de confianza si la dirección no está incluida en la lista.

NOTA: Al conectar a la interfaz web del iDRAC con un certificado en el cual el explorador no confía, aparece por segunda vez la advertencia de error de certificado del explorador después de confirmar la primera advertencia. Éste es el comportamiento esperado para garantizar la seguridad.

Para agregar la dirección IP de iDRAC6 a la lista de los dominios de confianza en IE8, haga lo siguiente:

1. Seleccione **Herramientas→ Opciones de Internet→ Seguridad→ Sitios de confianza→ Sitios**.
2. Introduzca la dirección IP de iDRAC6 en **Agregar este sitio web a la zona**.
3. Haga clic en **Add** (Agregar).
4. Haga clic en **OK** (Aceptar).
5. Haga clic en **Close** (Cerrar).
6. Haga clic en **Aceptar** y actualice el explorador.

Al iniciar la consola virtual por primera vez a través de IE8 con el complemento Active-X, puede aparecer el mensaje "`Certificate Error: Navegación bloqueada`".

1. Haga clic en **Continuar a este sitio web**.
2. Haga clic en **Instalar** para instalar los controles Active-X en la ventana **Advertencia de seguridad**.

   Se inicia la sesión de consola virtual.

Cómo ver las versiones traducidas de la interfaz web

La interfaz web del iDRAC6 es compatible con los siguientes idiomas de sistema operativo:

- Inglés (en-us)
- Francés (fr)
- Alemán (de)
- Español (es)
- Japonés (ja)
- Chino simplificado (zh-cn)

Los identificadores ISO en paréntesis denotan la variantes de idiomas específicos admitidos. El uso de la interfaz con otros dialectos o idiomas no se admite y puede no funcionar como se desea. Para algunos idiomas admitidos, es posible que se deba ajustar el tamaño de la ventana del explorador a 1024 píxeles de ancho para visualizar todas las funciones.

La interfaz web del iDRAC6 está diseñada para funcionar con teclados localizados para las variantes de idiomas específicos mencionados anteriormente. Algunas funciones de la interfaz web del iDRAC6, como la consola virtual, pueden requerir pasos adicionales para acceder a algunas funciones o letras. Para más detalles sobre cómo usar su teclado localizado en estos casos, ver "Uso de Video Viewer" en la página 237. El uso de otros teclados no es compatible y puede causar problemas inesperados.

NOTA: Consulte la documentación del explorador que indica cómo configurar diferentes idiomas y visualizar versiones localizadas de la interfaz web del iDRAC6.

Cómo establecer la configuración regional en Linux

El visor de consola virtual requiere un conjunto de caracteres UTF-8 para mostrarse correctamente. Si la pantalla no es legible, revise la configuración local y, si es necesario, restablezca el conjunto de caracteres.

Para establecer el conjunto de caracteres en un cliente Linux con una interfaz gráfica de usuario en chino simplificado:

1 Abra una terminal de comandos.

2 Escriba `locale` y presione <Intro>. Se mostrará un resultado similar al siguiente:

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3 Si los valores incluyen `zh_CN.UTF-8`, no será necesario hacer cambios. Si los valores no incluyen `zh_CN.UTF-8`, vaya al paso 4.

4 Modifique el archivo **/etc/sysconfig/i18n** con un editor de textos.

5 En el archivo, aplique los cambios siguientes:

Entrada actual:

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

Entrada actualizada:

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.UTF-
8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
```

6 Cierre la sesión e inicie sesión en el sistema operativo.

Cuando cambie de cualquier otro idioma, compruebe que este ajuste siga siendo válido. Si no es así, repita este procedimiento.

Desactivación de la función de lista blanca en Firefox

Firefox tiene una función de seguridad denominada "lista blanca" que requiere permiso del usuario para instalar complementos para cada sitio distinto que aloje un complemento. Cuando está activada, la función de lista blanca requiere que se instale un visor de consola virtual por cada iDRAC6 que se visite, aunque las versiones del visor sean idénticas.

Para desactivar la función de lista blanca y evitar la instalación innecesaria de complementos, realice los pasos a continuación:

1. Abra una ventana del explorador de web Firefox.
2. En el campo de dirección, escriba `about:config` y presione <Intro>.
3. En la columna **Nombre de la preferencia**, localice **xpinstall.whitelist.required** y haga clic en éste.

   Los valores de **Nombre de la preferencia**, **Estado**, **Tipo** y **Valor** cambian a texto en negritas. El valor **Estado** cambia a **establecido por el usuario** y el valor de **Valor** cambia a **false**.
4. En la columna **Nombre de la preferencia**, localice **xpinstall.enabled**.

   Asegúrese de que **Valor** sea **true**. Si no lo es, haga doble clic en **xpinstall.enabled** para cambiar el **Valor** a **true**.

Instalación del software del iDRAC6 en la estación de administración

El sistema incluye el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management). Este DVD incluye los siguientes componentes:

- Directorio raíz del DVD: contiene la utilidad Dell Systems Build and Update, que brinda información sobre la instalación y configuración del servidor y del sistema.
- SYSMGMT: contiene productos de software de administración de sistemas, incluido Dell OpenManage Server Administrator

Instalación y desinstalación de RACADM en una estación de administración

Para usar las funciones remotas de RACADM, instale RACADM en una estación de administración. Consulte la *Dell OpenManage Management Station Software Installation Guide* (Guía de instalación de Dell OpenManage Management Station Software) disponible en **dell.com/support/manuals** para obtener más información acerca de la instalación de DRAC Tools en una estación de administración con sistema operativo de Microsoft Windows.

Instalación y desinstalación de RACADM en Linux

1. Inicie sesión como usuario "root" en el sistema en donde desea instalar los componentes de la estación de administración.
2. De ser necesario, monte el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) con el comando siguiente o un comando similar:

   ```
   mount /media/cdrom
   ```

3. Diríjase al directorio **/linux/rac** y ejecute el comando siguiente:

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

Para obtener ayuda con el comando RACADM, escriba **racadm help** después de enviar los comandos anteriores.

Para desinstalar RACADM, abra un símbolo del sistema y escriba:

```
rpm -e <nombre_del_paquete_de_racadm>
```

donde `<racadm_package_name>` es el paquete RPM que se usó para instalar el software del iDRAC6.

Por ejemplo, si el nombre del paquete RPM es **srvadmin-racadm5**, escriba:

```
rpm -e srvadmin-racadm5
```

Instalación de Java Runtime Environment (JRE)

NOTA: Si usa el explorador Internet Explorer, se ofrece un control ActiveX para el visor de consola virtual. También puede usar el visor de consola virtual de Java con Firefox si instala JRE y configura el visor de consola virtual en la interfaz web del iDRAC6 antes de iniciar el visor. Ver "Configuración de la consola virtual y los medios virtuales en la interfaz web del iDRAC6" en la página 232 para obtener más información.

Usted puede optar por usar el visor de Java antes de iniciar el visor.

Si usa el explorador Firefox deberá instalar un JRE (o un paquete de desarrollo de Java [JDK]) para usar la función de consola virtual. El visor de consola virtual es una aplicación de Java que se descarga en la estación de administración desde la interfaz web del iDRAC6 y después se inicia con Java Web Start en la estación de administración.

Vaya a **java.com** para instalar JRE o JDK. Se recomienda la versión 1.6 (Java 6.0) o versiones superiores.

El programa Java Web Start se instala automáticamente junto con el JRE o JDK. El archivo **jviewer.jnlp** se descarga a su escritorio y un cuadro de diálogo le pregunta qué acción realizar. Puede ser necesario asociar el tipo de extensión **.jnlp** con la aplicación Java Web Start en el explorador. De otro modo, elija la opción de **Abrir con** y después seleccione la aplicación javaws, que se encuentra en el subdirectorio bin del directorio de instalación de JRE.

NOTA: Si el tipo de archivo **.jnlp** no está asociado con Java Web Start después de instalar JRE o JDK, puede configurar la asociación manualmente. Para Windows **(javaws.exe)** haga clic en **Inicio→ Panel de control→ Apariencia y temas→ Opciones de carpeta**. En la ficha **Tipos de archivos**, marque **.jnlp** en **Tipos de archivo registrados** y después haga clic en **Cambiar**. Para Linux **(javaws)**, inicie Firefox y después haga clic en **Editar→ Preferencias→ Descargas** y después haga clic en **Acciones de visualización y edición**.

Para Linux, una vez que ha instalado JRE o JDK, agregue una ruta de acceso al directorio bin Java al frente de su RUTA DE ACCESO del sistema. Por ejemplo, si Java está instalado en /usr/java, agregue la siguiente línea a su local.bashrc o /etc/profil:

```
PATH=/usr/java/bin:$PATH; export PATH
```

NOTA: Es posible que los archivos ya contengan líneas de modificación de RUTA DE ACCESO. Asegúrese de que la información de ruta de acceso no cree conflictos.

Instalación de clientes Telnet o SSH

De manera predeterminada, el servicio Telnet del iDRAC6 está desactivado y el servicio SSH está activado. Como Telnet es un protocolo inseguro, sólo debe usarse cuando no se puede instalar un cliente SSH o la conexión de red tiene otro tipo de seguridad.

NOTA: El iDRAC6 admite un máximo de 4 sesiones de Telnet y 4 sesiones de SSH de forma simultánea.

Telnet con iDRAC6

El cliente Telnet se incluye en los sistemas operativos Windows y Linux y se puede ejecutar desde un shell de comandos. También puede optar por instalar un cliente Telnet comercial o gratuito con más funciones prácticas que la versión estándar que se incluye en el sistema operativo.

Configuración de la tecla de retroceso para las sesiones de Telnet

El uso de la tecla <Retroceso> puede producir resultados inesperados, según el cliente Telnet. Por ejemplo, la sesión puede mostrar el eco `^h`. Sin embargo, la mayoría de los clientes Telnet de Microsoft y Linux se pueden configurar para usar la tecla <Retroceso>.

Para configurar los clientes Telnet de Microsoft para que puedan usar la tecla <Retroceso>, realice los pasos que se indican a continuación:

1. Abra una ventana de símbolo del sistema (si es necesario).
2. Si no está ejecutando una sesión de Telnet, escriba:

   ```
   telnet
   ```

   Si está ejecutando una sesión de Telnet, presione <Ctrl><]>.
3. En el indicador, introduzca:

   ```
   set bsasdel
   ```

   Aparece el mensaje siguiente:

   ```
   El retroceso se procesará como eliminación.
   ```

Para configurar una sesión de Telnet de Linux para usar la tecla <Retroceso>, realice los pasos a continuación:

1. Abra un shell y escriba:

   ```
   stty erase ^h
   ```

2. En el indicador, introduzca:

   ```
   telnet
   ```

SSH con iDRAC6

Secure Shell (SSH) es una conexión de línea de comandos con las mismas capacidades que una sesión Telnet, pero con negociación de sesión y cifrado para mejorar la seguridad. El iDRAC6 admite la versión 2 de SSH con autentificación de contraseña. SSH está activado en el iDRAC6 de manera predeterminada.

Puede usar programas como PuTTY u OpenSSH en una estación de administración para conectarse al iDRAC6 del servidor administrado. Cuando se presenta un error durante el procedimiento de inicio de sesión, el cliente **SSH** envía un mensaje de error. El texto del mensaje está en función del cliente y no es controlado por el iDRAC6.

NOTA: `OpenSSH` se debe ejecutar desde un emulador de terminal VT100 o ANSI en Windows. La ejecución de `OpenSSH` en el símbolo del sistema de Windows no produce una funcionalidad completa (es decir, algunas teclas no responden y no se muestran gráficos).

El iDRAC6 admite un máximo de 4 sesiones de Telnet y 4 sesiones de SSH de forma simultánea. No obstante, sólo una de las 8 sesiones posibles puede utilizar SM-CLP. Es decir, el iDRAC6 admite solamente una sesión SM-CLP por vez. El tiempo de espera de la sesión está controlado por la propiedad `cfgSsnMgtSshIdleTimeout` según aparece descrito en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

La implementación de SSH del iDRAC6 admite varios esquemas de criptografía, según se muestra en Tabla 3-1.

NOTA: No se admite SSHv1.

Tabla 3-1. Esquemas de criptografía

Tipo de esquema	Esquema
Criptografía asimétrica	Diffie-Hellman DSA/DSS 512:1024 bits (aleatorios) 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
Autenticación	• Password

Instalación de un servidor TFTP

El Protocolo de transferencia de archivos trivial (TFTP) es una forma simplificada del Protocolo de transferencia de archivos (FTP). Se usa con las interfaces de línea de comandos de SM-CLP y RACADM para transferir archivos hacia y desde el iDRAC6.

NOTA: Si usa únicamente la interfaz web del iDRAC6 para transferir certificados de SSL y cargar un nuevo firmware al iDRAC6, no necesita un servidor TFTP.

Las únicas ocasiones en las que necesita copiar archivos desde o en el iDRAC6 surgen cuando actualiza el firmware del iDRAC6 o cuando instala certificados en el iDRAC6. Si decide usar RACADM cuando realice estas tareas, deberá tener un servidor TFTP funcionando en un equipo al que el iDRAC6 pueda tener acceso por medio de la dirección IP o del nombre DNS.

Puede usar el comando `netstat -a` en los sistemas operativos Windows o Linux para determinar si ya hay un servidor TFTP activo. El puerto 69 es el puerto predeterminado de TFTP. Si no hay un servidor funcionado, tiene las siguientes opciones:

- Encuentre otro equipo en la red que ejecute un servicio TFTP.
- Si usa Linux, instale un servidor TFTP a partir de su distribución.
- Si usa Windows, instale un servidor TFTP comercial o gratuito.

Instalación de Dell OpenManage IT Assistant

El sistema incluye el paquete de software Dell OpenManage System Management. Este paquete incluye, entre otros, los siguientes componentes:

- DVD *Dell Systems Management Tools and Documentation*
- Sitio web del servicio de asistencia Dell Support y archivos léame: consulte los archivos léame y el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para consultar la información más reciente sobre los productos Dell.

Para obtener más información acerca de cómo instalar IT Assistant, consulte la *Dell OpenManage IT Assistant User's Guide* (Guía del usuario de Dell OpenManage IT Assistant) disponible en **dell.com/support/manuals**.

Instalación de Dell Management Console

La consola de administración Dell (DMC) es la aplicación de próxima generación para la administración de uno a varios sistemas, que ofrece una funcionalidad similar a la de Dell OpenManage IT Assistant y también incluye funciones mejoradas de descubrimiento, inventario, supervisión e informes. Se trata de una interfaz gráfica de usuario basada en web que se instala en una estación de administración en un entorno de red.

Puede instalar DMC desde el DVD *Dell Management Console* o descargarla e instalarla desde el sitio web de Dell en **dell.com/openmanage**.

Consulte la *Dell Management Console User's Guide* (Guía del usuario de Dell Management Console) disponible en **dell.com/support/manuals** para consultar las instrucciones de instalación del software.

4

Configuración del servidor administrado

Esta sección describe las tareas para configurar el servidor administrado a fin de mejorar las capacidades de administración remota. Estas tareas incluyen la instalación del software Dell OpenManage Server Administrator y la configuración del servidor administrado para capturar la pantalla de último bloqueo.

Instalación del software en el servidor administrado

El software de administración de Dell incluye las siguientes funciones:

- Interfaz de línea de comandos de RACADM: Permite administrar y configurar el iDRAC6. Es una herramienta potente para efectuar tareas de configuración y administración de secuencias de comando.
- Server Administrator: Es necesario usar la función de pantalla de último bloqueo del iDRAC6.
- Server Administrator Instrumentation Service: Proporciona acceso a información detallada sobre fallas y rendimiento recopilada por agentes de administración de sistemas estándar de la industria, y permite la administración remota de sistemas supervisados, incluso acciones de apagado, inicio y seguridad.
- Server Administration Storage Management Service: Brinda información sobre administración de almacenamiento en una vista gráfica integrada.
- Registros de Server Administrator: Muestran registros de los comandos recibidos o enviados por el sistema, los sucesos de hardware supervisados, los sucesos de la POST y las alertas del sistema. Los registros se pueden ver en la página de inicio, imprimir o guardar como informes y enviarse por correo electrónico a un contacto de servicio designado.

Utilice el DVD *Dell Systems Management Tools and Documentation* (Documentación y y herramientas de Dell Systems Management Tools) para instalar Dell OpenManage Server Administrator. Para obtener las instrucciones para instalar este software, consulte la *Dell OpenManage Server Administrator Installation Guide* (Guía de instalación de Dell OpenManage Server Administrator) que se encuentra disponible en **dell.com/support/manuals**. En la página **Manuales**, haga clic en **Software→ Systems Management**. Haga clic en el vínculo del producto correspondiente que se encuentra a la derecha para tener acceso a los documentos.

Configuración del servidor administrado para capturar la pantalla de último bloqueo

El iDRAC6 puede capturar la pantalla del último bloqueo para que usted pueda verla en la interfaz web y tratar de solucionar la causa del bloqueo del servidor administrado.

NOTA: Puede capturar la pantalla del último bloqueo solamente si el servidor administrado se está ejecutando en el sistema operativo Windows.

Siga estos pasos para activar la función de pantalla del último bloqueo.

1. Instalación del software de servidor administrado. Para obtener más información, consulte la *Guía de instalación de Dell OpenManage Server Administrator* y la *Guía de instalación de Dell OpenManage Management Station Software*. Puede acceder a estos documentos en el sitio web del servicio de asistencia Dell Support en**dell.com/support/manuals**.
2. Asegúrese de que **Reiniciar automáticamete** está deseleccionado en **Configuración de inicio y recuperación de Windows**. Vea la "Desactivación de la opción de reinicio automático de Windows" en la página 87.
3. Active la **Pantalla de último bloqueo** (desactivada de manera predeterminada) en la interfaz web del iDRAC6.

   Para activar la **Pantalla de último bloqueo** en la interfaz web del iDRAC6, haga clic en **Sistema→ Configuración de iDRAC→ ficha Red/ Seguridad→ Servicios**, y, a continuación, haga clic en la casilla **Activado** que se encuentra bajo el encabezado **Configuración del agente de recuperación automática del sistema**.

Para activar la pantalla del último bloqueo por medio de RACADM local, abra un símbolo del sistema en el servidor administrado y escriba el comando siguiente:

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

4 En la interfaz web de Server Administrator, active el temporizador de **Recuperación automática** y configure la acción de **Recuperación automática** en **Restablecer**, **Apagar** o **Ciclo de encendido**.

Para obtener información acerca de la configuración del temporizador de **Recuperación automática**, consulte la *Guía del usuario de Server Administrator de Dell OpenManage*. Para asegurarse que la pantalla de último bloqueo se pueda guardar, el temporizador de **Recuperación automática** se deberá establecer en 60 segundos. El valor predeterminado es de 480 segundos.

La pantalla de último bloqueo no estará disponible cuando la acción de **Recuperación automática** se establezca en **Apagar** o **Ciclo de encendido** si el servidor administrado está apagado.

Desactivación de la opción de reinicio automático de Windows

Para asegurarse de que el iDRAC6 pueda capturar la pantalla del último bloqueo, desactive la opción **Reinicio automático** en los servidores administrados que ejecutan Windows Server o Windows Vista.

1 Abra el **Panel de control** de Windows y haga doble clic en el icono **Sistema**.

2 Haga clic en la ficha **Advanced** (Opciones avanzadas).

3 En **Inicio y recuperación**, haga clic en **Configuración**.

4 Deseleccione la casilla de verificación **Reiniciar automáticamente**.

5 Haga clic dos veces en **Aceptar**.

5

Configuración del iDRAC6 Enterprise por medio de la interfaz web

El iDRAC6 ofrece una interfaz web que permite configurar las propiedades y los usuarios del iDRAC6, realizar tareas de administración remota y solucionar problemas de un sistema (administrado) remoto. Por lo general, utilizará la interfaz web para realizar las tareas diarias de administración de sistemas. Este capítulo proporciona información acerca de la realización de tareas comunes de administración de sistemas con la interfaz web del iDRAC6 y proporciona vínculos a información relacionada.

La mayoría de las tareas de configuración para las que se utiliza la interfaz web también se pueden realizar con comandos de RACADM local o remoto o bien con comandos de SM-CLP.

Los comandos de RACADM local se ejecutan desde el servidor administrado. RACADM remoto es una utilidad cliente que se ejecuta en una estación de administración y utiliza la interfaz fuera de banda para comunicarse con el servidor administrado. Esta utilidad se utiliza con la opción **–r** para ejecutar los comandos a través de una red. Para obtener más información sobre un RACADM, consulte "Uso de la interfaz de línea de comandos de RACADM" en la página 289.

Los comandos de SM-CLP se ejecutan en un shell al que se puede tener acceso de manera remota con una conexión Telnet o Secure Shell (SSH). Para obtener más información acerca de SM-CLP, ver "Uso de la interfaz de línea de comandos SM-C LP de iDRAC6 Enterprise" en la página 333.

Acceso a la interfaz web

Para acceder a la interfaz web del iDRAC6, realice los pasos a continuación:

1. Abra una ventana de un explorador web compatible.
2. En el campo **Dirección**, escriba `https://<Dirección_IP_del_iDRAC6>` y presione <Intro>.

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

   `https://<dirección_IP_del_iDRAC6>:<número_de_puerto>`

   donde *dirección_IP_del_iDRAC6* es la dirección IP del iDRAC6 y *número_de_puerto* es el número del puerto HTTPS.

   Aparece la ventana **Inicio de sesión** del iDRAC6.

Inicio de sesión

Puede iniciar sesión como usuario del iDRAC6, como usuario de Microsoft Active Directory o como usuario del LDAP. El nombre predeterminado y la contraseña son **root** y **calvin**, respectivamente.

Para que pueda iniciar sesión en el iDRAC6, el administrador debe haberle otorgado privilegio de **Inicio de sesión en el iDRAC6**.

Para iniciar sesión, realice los pasos siguientes:

1. En el campo **Nombre de usuario**, escriba uno de los siguientes valores:
   - Su nombre de usuario del iDRAC6.

     NOTA: En el nombre de usuario para los usuarios locales se *distingue entre mayúsculas* y *minúsculas*. Algunos ejemplos son root, usuario_de_ti, usuario_de_TI o juan_perez.

   - Su nombre de usuario de Active Directory (AD). También puede seleccionar el nombre del dominio de AD del menú desplegable.

     Puede utilizar cualquiera de los siguientes formatos para los nombres de Active Directory: *<dominio>\<nombre_de_usuario>*, *<dominio>/<nombre_de_usuario>* o *<usuario>@<dominio>*. En ellos no se distingue entre mayúsculas y minúsculas. Algunos ejemplos son `dell.com\juan_perez` o `JUAN_PEREZ@DELL.COM`. Como alternativa, puede introducir el dominio en el campo **Dominio**.

   - Nombre de usuario de LDAP (sin nombre de dominio).

2 En el campo **Contraseña**, introduzca su contraseña de usuario del iDRAC6, su contraseña de usuario de Active Directory o su contraseña del LDAP. Las contraseñas distinguen entre mayúsculas y minúsculas.

3 Haga clic en **Aceptar** o presione <Intro>.

Cierre de sesión

1 En la esquina superior derecha de la ventana principal, haga clic en **Cerrar sesión** para cerrar la sesión.

2 Cierre la ventana del explorador.

NOTA: El botón **Cerrar sesión** no aparecerá a menos que usted haya iniciado sesión.

NOTA: Cerrar el explorador sin desconectarse como corresponde puede hacer que la sesión permanezca activa hasta que expire el tiempo de la misma. Se recomienda que haga clic en el botón **Cerrar sesión** para finalizar una sesión.

NOTA: Si se cierra la interfaz web del iDRAC6 en Internet Explorer mediante el botón para cerrar ("x"), que se encuentra en la esquina superior derecha de la ventana, podría generarse un error de aplicación. Para resolver este problema, descargue la actualización de seguridad acumulativa más reciente para Internet Explorer desde el sitio web de asistencia de Microsoft, en **support.microsoft.com**.

PRECAUCIÓN: Si ha abierto múltiples sesiones de la interfaz web de usuario mediante <Ctrl+T> o <Ctrl+N> para acceder al mismo iDRAC6 desde una misma estación de administración y, a continuación, cierra alguna de las sesiones, todas finalizarán.

Uso de varias fichas y ventanas del explorador

Versiones diferentes de exploradores web se comportan de distinta manera al abrir nuevas fichas y ventanas. Internet Explorer (IE) 7 e IE 8 ofrecen la opción de abrir fichas además de ventanas. Cada ficha hereda las características de la última ficha abierta. Presione `<Ctrl-T>` para abrir una nueva ficha y `<Ctrl-N>` para abrir una nueva ventana del explorador desde la sesión activa. El inicio de sesión automático solamente se lleva a cabo con <Ctrl-N>. Cuando abra una nueva ficha, tendrá que iniciar sesión nuevamente. Al cerrar una ficha finalizan todas las fichas de interfaz Web de iDRAC6. Asimismo, si un usuario inicia sesión con privilegios de usuario avanzado en una ficha y después inicia sesión como Administrador en otra ficha, ambas fichas abiertas tendrán privilegios de administrador.

El comportamiento de las fichas en Firefox 3 es igual que en IE 7 e IE 8; nuevas fichas inician nuevas sesiones. Sin embargo, el comportamiento de las ventanas en Firefox es diferente. Las ventanas de Firefox operan con los mismos privilegios de la última ventana abierta. Por ejemplo, si una ventana de Firefox se abre con la sesión de un usuario avanzado y se abre otra ventana con privilegios de administrador, **ambos** usuarios tendrán privilegios de administrador.

Tabla 5-1. Comportamiento de los privilegios de usuario en exploradores admitidos

Explorador	Comportamiento de las fichas	Comportamiento de las ventanas
Microsoft IE 7 y 8	Desde la última sesión abierta	Nueva sesión
Firefox 3	Desde la última sesión abierta	Desde la última sesión abierta

Configuración del NIC del iDRAC6

Esta sección supone que el iDRAC6 ya ha sido configurado y está accesible' en la red. Ver "Configurar el sistema de red del iDRAC6" en la página 37 para obtener ayuda con la configuración inicial de la red del iDRAC6.

Configuración de los valores de VLAN, de IPMI y de red

NOTA: Para realizar los pasos a continuación, se debe tener privilegio para **Configurar el iDRAC6**.

NOTA: La mayoría de los servidores DHCP requiere un servidor para guardar un testigo identificador de cliente en la tabla de reservaciones. El cliente (por ejemplo, el iDRAC6) debe proporcionar este testigo durante la negociación de DHCP. El iDRAC6 proporciona la opción de identificador de cliente con un número de interfaz de un byte (0) seguido de una dirección MAC de seis bytes.

1. Haga clic en **Sistema→ Configuración de iDRAC**.
2. Haga clic en la ficha **Red/Seguridad**.

   Se muestra la pantalla **Red**.
3. Configure la red, IPMI y VLAN según sea necesario. Ver la Tabla 5-2, la Tabla 5-3 y la Tabla 5-4 para ver descripciones de las opciones de configuración de **red, IPMI** y **VLAN**.

4 Haga clic en **Aplicar**.

5 Para continuar, haga clic en el botón correspondiente.

Tabla 5-2. Configuración de red

Valor	Descripción
Configuración de tarjeta de interfaz de red	
Dirección MAC	Muestra la dirección de control de acceso al medio (MAC) que identifica de manera exclusiva a cada uno de los nodos de una red. La dirección MAC no se puede cambiar.
Activar la NIC	Cuando se selecciona, indica que la NIC está activada y activa los controles restantes en este grupo. Cuando el NIC está desactivado, se bloquea toda la comunicación con el iDRAC6 a través de la red. El valor predeterminado es **Deseleccionado**.
Valores comunes	
Registrar iDRAC6 en el DNS	Registra el nombre del iDRAC6 en el servidor DNS. El valor predeterminado es **Deseleccionado**.
iDRAC6 en DNS Name (Nombre)	Muestra el nombre del iDRAC6. El nombre predeterminado es idrac-*etiqueta_de_servicio*, donde *etiqueta_de_servicio* es el número de la etiqueta de servicio del servidor Dell. Por ejemplo: iDRAC-HM8912S.
Utiliza DHCP para el nombre del dominio de DNS	**Seleccionado**: se activa la adquisición del nombre de dominio de DNS desde el servidor DHCP. **No seleccionado**: se desactiva la adquisición del nombre de dominio de DNS desde el servidor DHCP.
Nombre de dominio de DNS	El **nombre de dominio de DNS** predeterminado está en blanco. Cuando la casilla de verificación **Usar DHCP para el nombre de dominio DNS** está seleccionada, esta opción aparece en gris y el campo no se puede modificar.
Configuración de IPv4	
Activado	Activa (**Seleccionado**) o desactiva (**Deseleccionado**) la compatibilidad con el protocolo IPv4. La opción **Activar el NIC** debe estar seleccionada para activar este valor.

Tabla 5-2. Configuración de red *(continuación)*

Valor	Descripción
Activar DHCP	Si está **seleccionado**, Server Administrator obtiene la dirección IP para el NIC del iDRAC6 desde el servidor DHCP. También desactiva los campos **Dirección IP**, **Máscara de subred** y **Puerta de enlace**.
Dirección IP	Permite introducir o editar una dirección IP estática para el NIC del iDRAC6. Para cambiar este valor, deseleccione la opción **Activar DHCP**.
Máscara de subred	Permite introducir o editar una máscara de subred para el NIC del iDRAC6. Para cambiar este valor, deseleccione la opción **Activar DHCP**.
predeterminada	Permite introducir o editar una puerta de enlace estática IPv4 para el NIC del iDRAC6. Para cambiar este valor, deseleccione la opción **Activar DHCP**.
Use DHCP para obtener direcciones del servidor DNS	Seleccione la opción **Activar DHCP** para obtener direcciones de servidores DNS al seleccionar la casilla de verificación **Usar DHCP para obtener direcciones de servidor DNS**. Cuando no se use el DHCP para obtener las direcciones de servidores DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.
Servidor DNS preferido	Permite introducir o editar una dirección IP estática para el servidor DNS preferido. Para cambiar este valor, deseleccione primero la opción **Usar DHCP para obtener direcciones de servidor DNS**.
Servidor DNS alternativo	Utiliza la dirección IP del servidor DNS secundario cuando la opción **Usar DHCP para obtener direcciones de servidor DNS no está seleccionada**. Introduzca una dirección IP 0.0.0.0 si no hay ningún servidor DNS alternativo.
Configuración de IPv6	
Activado	Si la casilla de verificación está **seleccionada**, IPv6 está activado. Si la casilla de verificación **no está seleccionada**, IPv6 está desactivado. El valor predeterminado es **Deseleccionado**.

Tabla 5-2. Configuración de red *(continuación)*

Valor	Descripción
Activar configuración automática	Seleccionar esta opción le permite al iDRAC6 obtener la dirección IPv6 para el NIC del iDRAC6 desde el servidor del Protocolo de configuración dinámica de host (DHCPv6). Al activar **Activar configuración automática** también se desactivan y vacían los valores estáticos para **Dirección IPv6**, **Longitud de prefijo** y **Puerta de enlace**.
Dirección IPv6	Configura la dirección IPv6 para el NIC del iDRAC6. Para cambiar estos valores, primero debe desactivar la opción **Activar configuración automática** deseleccionando la casilla de verificación relacionada. **NOTA:** Sólo dos direcciones IPv6 (la dirección de vínculo local y la dirección global) se muestran si la configuración de la red tiene definido DHCP IPv6 y las dieciséis direcciones IPv6 se mostrarán si configuró el enrutador de red para enviar mensajes de anuncios del enrutador. **NOTA:** iDRAC6 no permite guardar la configuración si introduce una dirección IPv6 que conste de más de ocho grupos.
Longitud del prefijo	Configura la longitud de prefijo de la dirección IPv6. Puede tener un valor entre 1 y 128 inclusive. Para cambiar estos valores, primero debe desactivar la opción **Activar configuración automática** deseleccionando la casilla de verificación relacionada.
predeterminada	Configura la puerta de enlace IPv6 estática para el NIC del iDRAC6. Para cambiar estos valores, primero debe desactivar la opción **Activar configuración automática** deseleccionando la casilla de verificación relacionada.
Utilice el DHCPv6 para obtener direcciones de servidor DNS	Active el DHCP para obtener direcciones de servidor DNS IPv6 seleccionando la casilla de verificación **Usar DHCPv6 para obtener direcciones de servidor DNS**. Cuando no se usa DHCP para obtener las direcciones de servidores DNS, proporcione las direcciones IP en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**. El valor predeterminado es **deseleccionado**. **NOTA:** Cuando la casilla de verificación **Usar DHCPv6 para obtener direcciones de servidor DNS** esté seleccionada, las direcciones IP no se podrán introducir en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.

Tabla 5-2. Configuración de red *(continuación)*

Valor	Descripción
Servidor DNS preferido	Especifica la dirección IPv6 estática del servidor DNS preferido. Para cambiar este valor, deseleccione **Usar DHCPv6 para obtener direcciones de servidor DNS**.
Servidor DNS alternativo	Especifica la dirección IPv6 estática del servidor DNS alternativo. Para cambiar este valor, deseleccione **Usar DHCPv6 para obtener direcciones de servidor DNS**.

Tabla 5-3. Configuración de IPMI

Valor	Descripción
Activar IPMI en la LAN	Cuando está seleccionado, indica que el canal LAN de IPMI está activado. El valor predeterminado es **Deseleccionado**.
Límite del nivel de privilegios del canal	Configura el nivel máximo de privilegios del usuario que se puede aceptar en el canal de LAN. Seleccione una de las siguientes opciones: **Administrador, Operador** o **Usuario**. El valor predeterminado es **Administrador**.
Clave de cifrado	Configura la clave de cifrado. La clave de cifrado debe consistir en un número par de caracteres hexadecimales con un máximo de 40 caracteres sin espacios. La clave de cifrado predeterminada de IPMI sólo contiene ceros.

Tabla 5-4. Configuración de VLAN

Botón	Descripción
Activar identificación de VLAN	**Sí**: activada. **No**: desactivada. Si esta opción está activada, sólo se aceptará el tráfico con identificación de LAN virtual (VLAN) que coincida. **NOTA:** La configuración de VLAN sólo puede definirse a través de la interfaz web del CMC. El iDRAC6 sólo muestra el estado actual de activación; no puede modificar los valores en esta pantalla.
Id. de VLAN	Campo Identificación de VLAN de campos de 802.1g. Muestra un valor de 1 a 4094, excepto de 4001 a 4020.

Tabla 5-4. Configuración de VLAN *(continuación)*

Botón	Descripción
Priority	Campo Prioridad de campos de 802.1g. Este campo se utiliza para determinar la prioridad de la identificación de VLAN y muestra un valor de 0 a 7 para el nivel de prioridad de VLAN.

Tabla 5-5. Botones de configuración de la red

Botón	Descripción
Advanced Settings (Configuración avanzada)	Muestra la pantalla **Seguridad de la red**, lo que permite al usuario introducir atributos de rango de IP y bloqueo de IP.
Aplicar	Guarda todos los nuevos valores que se hayan introducido en la pantalla de configuración de la red. **NOTA:** Los cambios en la configuración de la dirección IP del NIC cierran todas las sesiones de usuario, por lo tanto, los usuarios deben volver a conectarse a la interfaz web del iDRAC6 con la configuración actualizada de la dirección IP. Todos los demás cambios requieren que se restablezca la tarjeta de interfaz de red, lo que provocará una breve pérdida de conectividad.

Configuración del filtrado de IP y bloqueo de IP

NOTA: Para realizar los pasos a continuación, se debe tener privilegio para **Configurar el iDRAC6**.

1. Haga clic en **Sistema→ Configuración de iDRAC**.
2. Haga clic en la ficha **Red/Seguridad**.

   Se muestra la pantalla **Red**.
3. Haga clic en **Configuración avanzada**.

   Se muestra la pantalla **Seguridad de la red**.
4. Configure los valores de filtro y bloqueo de IP, según sea necesario. Ver Tabla 5-6 para obtener descripciones de los valores de filtro y bloqueo de IP.
5. Haga clic en **Aplicar** para guardar los valores.

Tabla 5-6. Configuración de filtrado y bloqueo de IP

Valor	Descripción
Rango de IP activado	Activa la función de revisión del rango IP, que define un rango de direcciones IP que pueden acceder al iDRAC6. El valor predeterminado es **Desactivado**.
Dirección del rango de IP	Determina la dirección de subred IP aceptable. El valor predeterminado es **192.168.1.0**.
Máscara de subred del rango de IP	Define las posiciones significativas de bit en la dirección IP. La máscara de subred debe estar en formato de máscara de red, donde los bits más significativos son todos los números 1 con una sola transición a sólo ceros en los bits de orden inferior. El valor predeterminado es **255.255.255.0**.
Bloqueo de IP activado	Activa la función de bloqueo de dirección IP, lo que limita el número de intentos fallidos de inicio de sesión provenientes de una dirección IP específica durante un periodo predefinido. El valor predeterminado es **Desactivado**.
Número de fallas de bloqueo de IP	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión de la misma dirección. El valor predeterminado es **10**.
Ventana de fallas de bloqueo de IP	Determina el plazo en segundos durante el cual deben ocurrir el número de errores por fallos de bloque de IP para activar el tiempo de penalización de bloqueo de IP. El valor predeterminado es **3600**.
Tiempo de penalización de bloqueo de IP	El período en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas. El valor predeterminado es **3600**.

Configuración de los sucesos de plataforma

La configuración de sucesos de plataforma ofrece un mecanismo para configurar el iDRAC6 a fin de realizar las acciones seleccionadas ante ciertos mensajes de sucesos. Las acciones incluyen reiniciar el sistema, sin acción, realizar ciclo de encendido del sistema, apagar el sistema y generar una alerta (captura de sucesos de plataforma [PET] y/o correo electrónico).

Los sucesos de plataforma que se pueden filtrar se muestran en la Tabla 5-7.

Tabla 5-7. Sucesos de plataforma que se pueden filtrar

Índice	Suceso de plataforma
1	Filtro de aserción de advertencia de batería
2	Filtro de aserción de batería crítica
3	Filtro de aserción de voltaje crítico
4	Filtro de aserción de advertencia de temperatura
5	Filtro de aserción de temperatura crítica
6	Filtro de aserción de procesador crítico
7	Filtro de aserción de advertencia de procesador
8	Filtro de aserción de registro de eventos crítico
9	Filtro de aserción de vigilancia crítica
10	Filtro de aserción de advertencia de medio flash extraíble
11	Filtro de aserción informativa de medio flash extraíble ausente
12	Filtro de aserción de medio flash extraíble crítico
13	Filtro de redundancia perdida
14	Filtro de aserción crítica de administración de clave

Cuando se presenta un suceso de plataforma (por ejemplo, una *Advertencia de sonda de batería*), se genera un suceso del sistema que se registra en el registro de sucesos del sistema (SEL). Si este suceso coincide con un filtro de sucesos de plataforma (PEF) que está activado y se ha configurado el filtro para que genere una alerta (PET o correo electrónico), entonces se envía una alerta por correo electrónico o PET a uno o más destinos configurados.

Si el mismo filtro de sucesos de plataforma también está configurado para realizar una acción (por ejemplo, reiniciar el sistema), la acción se ejecuta.

Configuración de filtros de sucesos de plataforma (PEF)

NOTA: Configure los filtros de sucesos de plataforma antes de configurar la captura de sucesos de plataforma o las alertas por correo electrónico.

1. Inicie sesión en la interfaz web del iDRAC6.
2. Haga clic en **Sistema** y luego en la ficha **Administración de alertas**.

   Aparecerá la pantalla **Sucesos de plataforma**.
3. Seleccione la casilla de verificación de marcación **Activar alertas de filtro de sucesos de plataforma**. Debe seleccionar esta opción para poder enviar cualquier alerta de la plataforma a un destino válido.
4. Seleccione una de las siguientes acciones que desea activar para cada suceso.
   - Reiniciar sistema: cuando se produce un suceso, el sistema se reinicia (reinicio mediante sistema operativo).
   - Realizar ciclo de encendido del sistema: cuando se produce un suceso, el sistema se cierra, se apaga y se reinicia (reinicio mediante suministro de energía).
   - Apagar el sistema: cuando se produce un suceso, el sistema se cierra y se apaga.
   - Sin acción: cuando se produce un suceso, no se realiza ninguna acción. Éste es el valor predeterminado de un suceso.
5. Seleccione la opción **Generar alerta** al lado de cada suceso para el que desee generar una alerta.

NOTA: Puede activar o desactivar la generación de alertas para todos los sucesos mediante la selección o deselección de la casilla de verificación junto al encabezado de la columna **Generar alerta**.

6. Haga clic en **Aplicar**.

Configuración de capturas de sucesos de plataforma (PET)

NOTA: Debe tener permiso para **Configurar el iDRAC** para agregar, activar o desactivar una alerta SNMP. Las opciones siguientes no estarán disponibles si no se tiene permiso de **Configurar el iDRAC**.

1. Inicie sesión en la interfaz web del iDRAC6.
2. Compruebe que siguió los procedimientos descritos en "Configuración de filtros de sucesos de plataforma (PEF)" en la página 100.
3. Haga clic en **Sistema** y luego en la ficha **Administración de alertas**.

   Aparecerá la pantalla **Sucesos de plataforma**.

4 Haga clic en **Valores de captura**.

Aparecerá la pantalla **Valores de captura.**

5 Configure la dirección IP de destino de la PET:

a Seleccione la casilla de verificación de marcación **Activado** junto al **Número de destino** que desea activar.

b Introduzca una dirección IP en el cuadro correspondiente **Dirección IP de destino** IPv4 o IPv6.

c Haga clic en **Aplicar**.

NOTA: Para enviar una captura correctamente, configure el valor de **Cadena de comunidad**. El valor de **Cadena de comunidad** indica la cadena de comunidad que se va a utilizar en una captura de alertas de Protocolo simple de administración de red (SNMP) enviada desde el iDRAC6. Las capturas de alertas SNMP son transmitidas por el iDRAC6 cuando ocurre un suceso de plataforma. El valor predeterminado de la **Cadena de comunidad** es **Public**.

d Haga clic en **Enviar** para probar la alerta configurada.

e Para agregar una dirección IP de destino adicional, repita del paso a al paso d. Puede especificar hasta cuatro direcciones de destino IPv4 y cuatro IPv6.

Configuración de alertas por correo electrónico

1 Inicie sesión en la interfaz web del iDRAC6.

2 Compruebe que siguió los procedimientos descritos en "Configuración de filtros de sucesos de plataforma (PEF)" en la página 100.

3 Haga clic en **Sistema** y luego en la ficha **Administración de alertas**.

Aparecerá la pantalla **Sucesos de plataforma**.

4 Haga clic en **Configuración de alertas de correo electrónico**.

Aparecerá la pantalla **Configuración de las alertas por correo electrónico**.

5 Configure el destino de la alerta por correo electrónico.

a Seleccione la casilla de verificación **Activada** para la primera alerta de correo electrónico sin definir.

b Introduzca una dirección de correo electrónico válida en el campo **Dirección de correo electrónico de destino**.

c Haga clic en **Aplicar**.

NOTA: Para enviar correctamente un correo electrónico de prueba, el servidor SMTP (correo electrónico) debe estar configurado en la sección **Configuración de dirección del servidor SMTP (correo electrónico)** de la pantalla **Configuración de las alertas por correo electrónico**. Especifique un servidor SMTP en el campo provisto utilizando el formato de números separados por puntos (por ejemplo: 192.168.1.1) o el nombre DNS. Cuando tiene lugar un suceso de plataforma, la dirección IP del servidor SMTP envía alertas a iDRAC por correo electrónico.

d En el campo **Modificar nombre de correo electrónico de origen**, introduzca el correo electrónico iniciador del alerta, o bien deje el campo en blanco para utilizar el correo electrónico iniciador predeterminado. El correo predeterminado es blade_slot@iDRAC6 IP Address.

- Si el campo **Modificar nombre de correo electrónico de origen** está en blanco, el nombre del host del iDRAC6 está configurado y el nombre del dominio DNS está activo, entonces la dirección de correo electrónico de origen es: <iDRAC6 host name>@ <DNS Domain name>.
- Si el campo está en blanco, el nombre del host del iDRAC6 está en blanco y el nombre del dominio DNS está activo, entonces la dirección de correo electrónico de origen es: <iDRAC6 Slot*x*>@ <DNS Domain name>.
- Si el campo está en blanco, el nombre de host del iDRAC6 está en blanco y el nombre del dominio DNS está en blanco, entonces la dirección de correo electrónico de origen es: <iDRAC6 Slot*x*>@ <iDRAC6 IP Address>.
- Si el campo es “una cadena sin @” y el nombre del dominio DNS está activa, entonces la dirección de correo electrónico de origen es: <a string without @>@<DNS Domain name>.

- Si el campo es “una cadena sin @” y el nombre del dominio DNS está en blanco, entonces la dirección de correo electrónico de origen es: <a string without @>@<iDRAC6 IP Address>.
- Si el campo es “una cadena sin @” y el nombre del dominio DNS está activa, entonces la dirección de correo electrónico es: <a string with @>@<DNS Domain name>.
- Si el campo es “una cadena con @” y el nombre del dominio DNS está en blanco, entonces la dirección de correo electrónico de origen es: <a string with @>@<iDRAC6 IP Address>.

e Haga clic en **Enviar** para probar la alerta por correo electrónico configurada (si lo desea).

f Para agregar un destino de alertas por correo electrónico adicional, repita del paso a al paso e. Puede especificar hasta cuatro destinos de alertas por correo electrónico.

Configuración de IPMI en la LAN

1 Inicie sesión en la interfaz web del iDRAC6.

2 Configure la IPMI en la LAN:

a Haga clic en **Sistema→ Configuración de iDRAC**, y a continuación, haga clic en la ficha **Red/Seguridad** tab.

Se muestra la pantalla **Red**.

b Haga clic en **Configuración de IPMI**.

c Seleccione la casilla de verificación **Activar IPMI en la LAN**.

d Actualice el **Límite de nivel de privilegio del canal**, si es necesario:

NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones de IPMI 2.0.

En **Configuración de IPMI**, haga clic en el menú desplegable **Límite de nivel de privilegio del canal**, seleccione **Administrador**, **Operador** o **Usuario** y luego haga clic en **Aplicar**.

e Establezca la clave de cifrado del canal de LAN de IPMI, si es necesario.

NOTA: La IPMI del iDRAC6 es compatible con el protocolo RMCP+.

En **Configuración de IPMI**, en el campo **Clave de cifrado**, escriba la clave de cifrado.

f Haga clic en **Aplicar**.

3 Configure la comunicación en serie en la LAN (SOL) de IPMI.

a Haga clic en **Sistema→ Configuración de iDRAC**, y a continuación, haga clic en la ficha **Red/Seguridad** tab.

Se muestra la pantalla **Red**.

b Haga clic en la ficha **Comunicación en serie en la LAN**.

c Seleccione **Activar comunicación en serie en la LAN**.

d Si es necesario, actualice la **Velocidad en baudios** de SOL de IPMI seleccionando un valor en el menú desplegable **Velocidad en baudios**.

NOTA: Para redirigir la consola serie en la LAN, asegúrese de que la **Velocidad en baudios** de SOL sea idéntica a la velocidad en baudios del servidor administrado.

e Haga clic en **Aplicar**.

f Configure los valores de filtrado y bloqueo de IP según sea necesario en la página **Configuración avanzada**.

Cómo agregar y configurar usuarios del iDRAC6

Para administrar el sistema con el iDRAC6 y mantener la seguridad del sistema, cree usuarios únicos con permisos administrativos específicos (o con *autoridad basada en funciones*).

Para agregar y configurar usuarios del iDRAC6, realice los pasos siguientes:

NOTA: Para realizar los pasos siguientes, se debe tener permiso para **Configurar el iDRAC**.

1 Haga clic en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Usuarios**.

La pantalla **Usuarios** muestra la Identificación de usuario, Estado, Nombre del usuario, Privilegios de LAN de IPMI, Privilegios del iDRAC6 y Comunicación en serie en la LAN de cada usuario.

NOTA: El usuario 1 está reservado para el usuario anónimo de IPMI y no se puede configurar.

2 En la columna **Identificación de usuario**, haga clic en un número de identificación de usuario.

3 En la página **Menú principal de usuarios** (ver Tabla 5-8, Tabla 5-9 y Tabla 5-10), puede configurar un usuario, cargar un archivo de clave pública de SSH o ver o eliminar una clave específica o todas las claves de SSH.

Autentificación de la clave pública en el SSH

El iDRAC6 admite la autentificación de clave pública (PKA) a través de SSH. Este método de autentificación mejora la automatización de secuencias de comandos de SSH al eliminar la necesidad de incorporar o solicitar la identificación/contraseña del usuario.

Antes de comenzar

Puede configurar hasta 4 claves públicas *por usuario* que pueden ser utilizadas en la interfaz de SSH. Antes de agregar o eliminar claves públicas, no deje de utilizar el comando view para ver las claves que ya están configuradas y no sobrescribir ni eliminar accidentalmente una de ellas. Cuando la PKA en SSH está configurada y se utiliza correctamente, no es necesario que escriba la contraseña al iniciar sesión en el iDRAC6. Esto puede ser muy útil para configurar secuencias de comandos automatizadas para realizar distintas funciones.

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

- Puede administrar está función con RACADM y también con la GUI.
- Al agregar claves públicas nuevas, verifique que las claves existentes no se encuentren ya en el índice donde se agregará la clave nueva. iDRAC6 no realiza comprobaciones para verificar que las claves anteriores se han eliminado antes de agregar una nueva. Tan pronto se agrega una clave nueva, automáticamente entra en vigor siempre que la interfaz de SSH esté activada.

Generación de claves públicas para Windows

Antes de agregar una cuenta, se requiere una clave pública del sistema que accederá al iDRAC6 en el SSH. Hay dos maneras de generar el par de claves públicas/privadas: Mediante la aplicación *Generador de claves PuTTY* para clientes que ejecutan Windows o la CLI *ssh-keygen* para clientes que ejecutan Linux. La utilidad *ssh-keygen* de CLI está incluida de forma predeterminada en todas las instalaciones estándar.

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

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

1. Inicie la aplicación y seleccione SSH-2 RSA o SSH-2 DSA para el tipo de clave a generar. SSH-1 no es admitido.
2. Introduzca el número de bits para la clave. Los algoritmos admitidos para generar claves son RSA y DSA únicamente. El número tiene que estar entre los 768 y los 4096 bits para RSA y 1024 bits para DSA.
3. Haga clic en **Generar** y mueva el mouse dentro de la ventana como se indica. Después de crear la clave, se puede modificar el campo de comentario de la clave. También se puede introducir una frase contraseña para asegurar la clave. Verifique que ha guardado la clave privada.
4. Puede guardar la clave pública en un archivo utilizando la opción **Guardar clave pública** para cargarla más tarde. Todas las claves cargadas deben estar en formato RFC 4716 u openSSH. De lo contrario, deberá convertirlas a estos formatos.

Generación de claves públicas para Linux

La aplicación *ssh-keygen* para clientes Linux es una herramienta de línea de comandos sin interfaz gráfica de usuario.

Abra una ventana de terminal y en el indicador de shell introduzca:

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

NOTA: Las opciones distinguen entre mayúsculas y minúsculas.

donde,

-t puede 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.

Después de que el comando se ejecute, cargue el archivo público.

NOTA: Las claves generadas desde la estación de administración de Linux utilizando ssh-keygen no se encuentran en formato RFC4716, pero sí en openSSH. Las claves públicas en formato openSSH pueden ser cargadas en iDRAC6. El algoritmo para claves públicas iDRAC6 valida ambas claves, la openSSH y la RFC4716, internamente convierte las claves RFC4716 al formato openSSH y luego internamente las almacena.

NOTA: iDRAC6 no admite el envío ssh-agent de claves.

Inicio de sesión con autentificación de clave pública

Una vez que las claves públicas han sido cargadas, puede iniciar sesión en iDRAC6 en el SSH sin tener que introducir una contraseña. También tendrá la opción de enviar un solo comando de RACADM como argumento de línea de comandos a la aplicación de SSH. Las opciones de línea de comandos se comportan como RACADM remoto ya que la sesión finaliza al completarse el comando.

Por ejemplo,

Conectar:

```
nombre de usuario ssh@<dominio>
```

o

```
nombre de usuario ssh@<dirección_IP>
```

donde dirección_IP es la dirección IP del iDRAC6.

Envío de comandos RACADM:

```
nombre de usuario ssh@<dominio> racadm getversion
nombre de usuario ssh@<dominio> racadm getsel
```

Ver "Carga, visualización y eliminación de claves SSH usando RACADM" en la página 297 para obtener más información acerca de cómo cargar, ver y eliminar claves SSH utilizando RACADM.

Tabla 5-8. Configuraciones de claves SSH

Opción	Descripción
Cargar claves SSH	Permite al usuario local cargar un archivo de clave pública SSH. Si se carga una clave, el contenido del archivo de la clave aparece en un cuadro de texto no editable, en la página **Configuración del usuario**.
Ver/eliminar claves SSH	Permite al usuario local ver o eliminar una clave SSH especificada o todas las claves SSH.

La página **Cargar clave(s) SSH** le permite cargar un archivo de clave pública SSH. Si carga una clave, el contenido del archivo de la clave aparece en un cuadro de texto no editable en la página **Ver o quitar clave(s) SSH**.

PRECAUCIÓN: La capacidad de cargar, ver y/o eliminar claves SSH depende del privilegio de usuario "Configurar usuarios". Este privilegio les permite a los usuarios configurar la clave SSH de otro usuario. Se debe tener cuidado al otorgar este privilegio. Para obtener más información, consulte Tabla 5-13.

Tabla 5-9. Cargar clave(s) SSH

Opción	Descripción
Archivo o texto	Seleccione la opción **Archivo** y escriba la ruta de acceso donde se encuentra la clave. También puede seleccionar la opción **Texto** y copiar el contenido del archivo de la clave en el cuadro. Puede cargar nuevas claves o sobrescribir las existentes. Para cargar un archivo de clave, haga clic en **Explorar**, seleccione el archivo y haga clic en el botón **Aplicar**. **NOTA:** La opción Pegar texto de clave es admitida para claves públicas en el formato openSSH. La opción para pegar texto no está admitida para el formato RFC4716.
Examinar	Haga clic en este botón para ubicar la ruta de acceso completa y el nombre del archivo de la clave.

La página **Ver o quitar clave(s) SSH** le permite ver o quitar las claves públicas SSH del usuario.

Tabla 5-10. Ver o quitar clave(s) SSH

Opción	Descripción
Remove (Quitar)	En el cuadro aparece la clave cargada. Seleccione la opción **Quitar** y haga clic en **Aplicar** para eliminar la clave existente.

1. Si selecciona la opción **Configurar usuario** y hace clic en **Siguiente**, aparecerá la página **Configuración de usuario.**
2. En la pantalla **Configuración de usuario**, configure las propiedades y los privilegios de usuario.

   La Tabla 5-11 describe los valores **Generales** de configuración de un nombre de usuario y contraseña del iDRAC6.

La Tabla 5-12 describe los **Privilegios de LAN de IPMI** para configurar los privilegios de información acerca de LAN del usuario.

La Tabla 5-13 describe los permisos del **Grupo** de **usuarios** para la configuración de los **Privilegios de LAN de IPMI** y de los **Privilegios de usuario** del iDRAC6.

La Tabla 5-14 describe los permisos de **Grupo de iDRAC6**. Si agrega un **Privilegio de usuario del iDRAC6** al **Administrador**, **Usuario avanzado** o **Usuario invitado**, el **Grupo** de iDRAC6 cambiará a grupo **Personalizado**.

3 Una vez finalizado, haga clic en **Aplicar** para guardar la configuración.

Tabla 5-11. Propiedades generales

Propiedad	Descripción
Identificación de usuario	Contiene uno de los 16 números preconfigurados de identificación de usuario. Este campo no se puede editar.
Activar el usuario	Cuando está **seleccionado**, indica que el acceso del usuario al iDRAC6 está activado. Cuando **no está seleccionado**, el acceso del usuario está desactivado.
Nombre de usuario	Especifica un nombre de usuario del iDRAC6 de hasta 16 caracteres. Cada usuario debe tener un nombre de usuario exclusivo. • 0-9 • A-Z • A-Z • Caracteres especiales: + % = , - { § ! (? ; _ } I #) * : $ [| **NOTA:** Si el nombre de usuario se cambia, el nuevo nombre no aparecerá en la interfaz de usuario sino hasta el siguiente inicio de sesión del usuario.
Cambiar contraseña	Activa los campos **Contraseña nueva** y **Confirmar nueva contraseña**. Cuando está deseleccionada, la Contraseña del usuario no se puede cambiar.

Tabla 5-11. Propiedades generales *(continuación)*

Propiedad	Descripción
Contraseña nueva	Activa la edición de la contraseña del usuario del iDRAC6. Introduzca una **Contraseña** de hasta 20 caracteres. Los caracteres no se mostrarán. • 0-9 • A-Z • A-Z • Caracteres especiales: + % = , - { . ! (? ; _ } I | #) * : $ [/ @
Confirmar contraseña nueva	Vuelva a escribir la contraseña del usuario del iDRAC6 para confirmarla.

NOTA: iDRAC6 le permite crear nombres de usuario con los caracteres admitidos descritos en la tabla 5-12. Sin embargo, existen algunos caracteres de delimitador que no están admitidos en todas las interfaces de usuario como en la de RACADM. Los servicios de directorio también cuentan con restricciones relativas al formato del nombre de usuario.

Tabla 5-12. Privilegio LAN de IPMI

Propiedad	Descripción
Privilegio máximo permitido de usuario de LAN	Especifica el privilegio máximo del usuario en el canal de LAN de IPMI como uno de los siguientes grupos de usuario: **Ninguno**, **Administrador**, **Operador** o **Usuario**.
Activar comunicación en serie en la LAN.	Permite al usuario usar la comunicación en serie en la LAN de IPMI. Cuando está **seleccionado**, este privilegio está activado.

Tabla 5-13. Otro Privilegio

Propiedad	Descripción
Grupo del iDRAC6	Especifica el privilegio máximo del usuario de iDRAC6 como uno de los siguientes: **Administrador**, **Usuario avanzado**, **Usuario invitado**, **Personalizado** o **Ninguno**. Ver Tabla 5-14 para ver los permisos del **Grupo de iDRAC6**.
Iniciar sesión en el iDRAC6	Permite al usuario iniciar sesión en el iDRAC6.
Configurar el iDRAC6	Permite al usuario configurar el iDRAC6.
Configurar usuarios	Activa la capacidad del usuario de otorgar permisos de acceso al sistema a usuarios específicos. **PRECAUCIÓN: Este privilegio normalmente se reserva para usuarios que son miembros del grupo de usuarios Administrador de iDRAC. No obstante, se puede asignar este privilegio a los usuarios del grupo de usuarios "Personalizado". Un usuario con este privilegio puede modificar la configuración de cualquier usuario. Esto incluye la creación o eliminación de cualquier usuario, la administración de la clave SSH para usuarios, etc. Por estos motivos, asigne este privilegio con cuidado.**
Borrar registros	Permite al usuario borrar los registros del iDRAC6.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a la consola virtual	Permite al usuario ejecutar la consola virtual. **PRECAUCIÓN: Este privilegio normalmente se reserva para usuarios que son miembros del grupo de usuarios Avanzados o Administrador de iDRAC. Además de poder utilizar la consola virtual, los usuarios con el privilegio Acceder a la consola virtual tienen permiso para ver en la interfaz web del iDRAC6 las actividades de cualquiera que utilice la consola virtual. Por estos motivos, asigne este privilegio con cuidado.**
Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.

Tabla 5-13. Otro Privilegio *(continuación)*

Propiedad	Descripción
Probar alertas	Permite al usuario enviar alertas de prueba (por correo electrónico y PET) a todos los destinatarios de alertas actualmente configurados.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Tabla 5-14. Permisos de grupo del iDRAC6

Grupo de usuarios	Permisos otorgados
Administrador	Iniciar sesión en el iDRAC6, Configurar el iDRAC6, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico
Usuario avanzado	Iniciar sesión en el iDRAC6, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas
Usuario invitado	Iniciar sesión en el iDRAC6
Custom (Personalizar)	Selecciona cualquier combinación de los permisos siguientes: Iniciar sesión en el iDRAC6, Configurar el iDRAC6, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico
Ninguno	Sin permisos asignados

Cómo asegurar las comunicaciones del iDRAC6 por medio de certificados SSL y digitales

Esta sección ofrece información acerca de las siguientes funciones de seguridad de datos que vienen incorporadas en el iDRAC6:

- Capa de sockets seguros (SSL)
- Solicitud de firma de certificado (CSR)
- Acceso al menú principal de SSL

- Generación de una nueva CSR
- Carga de un certificado de servidor
- Visualización de un certificado de servidor

Capa de sockets seguros (SSL)

El iDRAC6 incluye un Web Server configurado para utilizar el protocolo de seguridad SSL (el estándar de la industria) para transferir datos cifrados a través de una red. Como está cimentada en la tecnología de cifrado de claves privada y pública, la SSL es una tecnología ampliamente aceptada para proporcionar comunicación cifrada y autentificada entre clientes y servidores a fin de prevenir el espionaje en una red.

Un sistema habilitado para SSL puede realizar las siguientes tareas:

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

El proceso de cifrado proporciona un alto nivel de protección de datos. El iDRAC6 emplea el estándar de cifrado SSL de 128 bits, la forma más segura de cifrado que está normalmente disponible para los exploradores de Internet en Norteamérica.

De manera predeterminada, el Web Server del iDRAC6 tiene un certificado digital SSL autofirmado (identificación del servidor) de Dell. Para garantizar una alta seguridad en Internet, sustituya el certificado SSL del Web Server por otro firmado por una autoridad de certificados (CA) de renombre. Una autoridad de certificados es una entidad comercial reconocida en el sector de tecnología informática por cumplir estándares altos de análisis confiable, identificación y otros criterios de seguridad importantes. Entre los ejemplos de autoridades de certificados se incluyen Thawte y VeriSign. Para iniciar el proceso de obtención de un certificado firmado, se puede utilizar la interfaz web del iDRAC6 para generar una solicitud de firma de certificado (CSR) con la información de la empresa. Usted podrá enviar entonces la solicitud CSR generada a una autoridad de certificados como VeriSign o Thawte.

Solicitud de firma de certificado (CSR)

Una CSR es una solicitud digital a una autoridad de certificados (CA) para obtener un certificado de servidor seguro. Los certificados de servidor seguro permiten a clientes del servidor confiar en la identidad del servidor y negociar una sesión cifrada con el servidor.

Una vez que la autoridad de certificación recibe una solicitud CSR, revisa y verifica la información que contiene. Si el solicitante cumple los estándares de seguridad, la autoridad de certificados emite un certificado firmado por soportes digitales que identifica al solicitante de forma exclusiva para transacciones a través de redes y en la Internet.

Después de que la autoridad de certificados apruebe la CSR y envíe el certificado, cargue el certificado en el firmware del iDRAC6. La información de la CSR almacenada en el firmware del iDRAC6 debe coincidir con la información que contiene el certificado, es decir, el certificado se tiene que haber generado en respuesta a la CSR creada por el iDRAC6.

Acceso al menú principal de SSL

1. Haga clic en **Sistema**→ **Configuración de iDRAC**→ ficha **Red/Seguridad**.
2. Haga clic en **SSL** para abrir la pantalla **SSL**.

La Tabla 5-15 describe las opciones disponibles al momento de generar una CSR.

Tabla 5-15. Opciones del menú principal de SSL

Campo	Descripción
Generar una nueva solicitud de firma de certificado (CSR)	Seleccione la opción y haga clic en **Siguiente** para abrir la pantalla **Generar solicitud de firma de certificado (CSR)**. Ver "Generación de una nueva solicitud de firma de certificado" en la página 115 para obtener más información. **NOTA:** Cada nueva CSR sobrescribirá los datos de la CSR anterior que esté guardada en el firmware. La información que el CSR contenga debe de coincidir con la información del certificado. De lo contrario, el iDRAC6 no aceptará el certificado.

Tabla 5-15. Opciones del menú principal de SSL *(continuación)*

Campo	Descripción
Cargar certificado de servidor	Seleccione la opción y haga clic en **Siguiente** para abrir la pantalla **Carga del certificado** y cargar el certificado que recibió de la autoridad de certificados. Ver "Carga de un certificado de servidor" en la página 116 para obtener más información. **NOTA:** El iDRAC6 sólo acepta certificados codificados con X509 v3, base 64. No acepta certificados codificados DER.
Ver el certificado de servidor	Seleccione la opción y haga clic en **Siguiente** para abrir la pantalla **Ver certificado del servidor** y acceder a un certificado de servidor existente. Ver "Cómo ver un certificado de servidor" en la página 117 para obtener más información.

Generación de una nueva solicitud de firma de certificado

NOTA: Cada nueva CSR sobrescribirá los datos de la CSR anterior que esté guardada en el firmware. La información que el CSR contenga debe de coincidir con la información del certificado. De lo contrario, el iDRAC6 no aceptará el certificado.

1. En la pantalla **SSL**, seleccione **Generar una nueva solicitud de firma de certificado (CSR)** y haga clic en **Siguiente**.
2. En la pantalla **Generar solicitud de firma de certificado (CSR)**, introduzca un valor para cada atributo de la CSR.

   La Tabla 5-16 describe las opciones de la pantalla **Generar solicitud de firma de certificado (CSR)**.
3. Haga clic en **Generar** para crear la CSR.
4. Haga clic en **Descargar** para guardar el archivo CSR en la estación de administración remota.

Tabla 5-16. Opciones para generar solicitud de firma de certificado (CSR)

Campo	Descripción
Nombre común	El nombre exacto que se certifica (por lo general, el nombre del dominio del servidor web, por ejemplo, **xyzcompany.com**). Se admiten todos los caracteres excepto '$'.
Nombre de la organización	El nombre asociado con esta organización (por ejemplo, Empresa XYZ). Se admiten todos los caracteres excepto '$'.

Tabla 5-16. Opciones para generar solicitud de firma de certificado (CSR) *(continuación)*

Campo	Descripción
Unidad organizacional	El nombre asociado con una unidad de organización, como un departamento (por ejemplo, Tecnología informática). Se admiten todos los caracteres excepto '$'.
Localidad	Ciudad u otra ubicación de la entidad que se está certificando (por ejemplo, Round Rock). Sólo son válidos los caracteres alfanuméricos y los espacios. No separe palabras con un guión bajo ni otro carácter.
Nombre del estado	El estado o provincia donde se encuentra la entidad que solicita una certificación (por ejemplo, Texas). Sólo son válidos los caracteres alfanuméricos y los espacios. No utilice abreviaturas.
Código del país	El nombre del país en el que se encuentra la entidad que solicita la certificación.
Correo electrónico	La dirección de correo electrónico asociada con la CSR. Escriba la dirección de correo electrónico de la empresa o cualquier dirección de correo electrónico asociada con la CSR. Este campo es opcional.
Tamaño de clave	El tamaño de la clave de solicitud de firma de certificado (CSR) que generará. El tamaño puede variar entre 1024 KB ó 2048 KB.

Carga de un certificado de servidor

1. En la pantalla **SSL**, seleccione **Cargar certificado de servidor** y haga clic en **Siguiente**.

   Aparecerá la pantalla **Carga del certificado**.

2. En el campo **Ruta del archivo,** haga clic en **Examinar** para ir hasta el certificado y especificar el archivo del certificado en la estación de administración.

   NOTA: El valor de la **Ruta del archivo** muestra la ruta del archivo del certificado que está cargando, que incluye la ruta completa, el nombre completo del archivo y la extensión del archivo.

3. Haga clic en **Aplicar** para cargar el certificado al firmware del iDRAC6.

Cómo ver un certificado de servidor

1 En la pantalla **SSL**, seleccione **Ver certificado del servidor** y haga clic en **Siguiente**.

La Tabla 5-17 describe los campos asociados con las descripciones que aparecen en la ventana **Ver certificado del servidor**.

Tabla 5-17. Ver información de certificado del servidor

Campo	Descripción
Serial Number (Número de serie)	Número de serie del certificado
Información del titular	Atributos del certificado introducidos por el titular
Información del emisor	Atributos del certificado generados por el emisor
Válido desde	Fecha de emisión del certificado
Válido hasta	Fecha de vencimiento del certificado

Configuración y administración de los certificados de Microsoft Active Directory

NOTA: Debe tener permiso para **Configurar el iDRAC** a fin de configurar Active Directory y cargar, descargar y ver un certificado de Active Directory.

NOTA: Para obtener más información acerca de la configuración de Active Directory y sobre cómo configurar Active Directory con el esquema estándar o un esquema ampliado, ver "Uso del servicio de directorio de iDRAC6" en la página 133.

Para acceder a la pantalla Resumen de **Microsoft Active Directory**, haga clic en **Sistema→ Configuración de iDRAC→ Red/Seguridad** ficha**→ Servicio de directorios→ Microsoft Active Directory**.

La Tabla 5-18 indica las opciones de resumen de **Active Directory**. Para continuar, haga clic en el botón correspondiente.

Tabla 5-18. Opciones de Active Directory

Campo	Descripción
Valores comunes	Muestra configuraciones frecuentes de Active Directory.
Certificado de CA de Active Directory	Muestra el certificado de la CA que firma todos los certificados de servidor SSL del controlador de dominio.
Configuración del esquema estándar/ Configuración del esquema ampliado	Según la configuración actual de Active Directory, se muestran la configuración del esquema ampliado o la configuración del esquema estándar.
Configurar Active Directory	Haga clic en esta opción para configurar el paso 1 de 4 de la configuración de Active Directory. La página **Paso 1 de 4 Active Directory** permite cargar un certificado de la autoridad de certificados (CA) de Active Directory al iDRAC6, ver el certificado actual de CA de Active Directory que se cargó al iDRAC6 o activar la validación de certificados.
Probar configuración	Haga clic en esta opción para verificar la configuración de Active Directory con las opciones especificadas.
Cargar archivo keytab de Kerberos	Haga clic en esta opción para cargar un archivo keytab de Kerberos en el iDRAC6. Para obtener información acerca de cómo crear un archivo keytab, ver "Configuración de iDRAC6 para el inicio de sesión único y mediante tarjeta inteligente" en la página 181.

Configuración de Active Directory (esquema estándar y esquema ampliado)

1. En la pantalla de resumen de **Active Directory**, haga clic en **Configurar Active Directory**.
2. En la pantalla **Paso 1 de 4 Active Directory**, puede activar la validación de certificados, cargar el certificado de CA de Active Directory en el iDRAC6 o ver el certificado de CA de Active Directory actual.

   La Tabla 5-19 describe la configuración y las selecciones para cada paso del proceso de **Configuración y administración de Active Directory**. Para continuar, haga clic en el botón correspondiente.

Tabla 5-19. Valores de configuración de Active Directory

Valor	Descripción
Paso 1 de 4 Configuración y administración de Active Directory	
Validación de certificados activada	Especifica si la validación de certificados está activada o desactivada. Si está **seleccionada**, la validación de certificados está activada. El iDRAC6 utiliza LDAP sobre la capa de sockets seguros (SSL) mientras se conecta a Active Directory. De manera predeterminada, al utilizar el certificado de la entidad emisora cargado en el iDRAC6, éste último proporciona una gran seguridad para validar el certificado del servidor SSL de los controladores de dominio durante el protocolo de enlace SSL. La validación de certificados se puede desactivar para fines de prueba.
Cargar certificado de CA de Active Directory	Para cargar un certificado de la entidad emisora de Active Directory, haga clic en **Examinar**, seleccione el archivo y haga clic en **Cargar**. Asegúrese de que los certificados SSL del controlador de dominio estén firmados por la misma entidad emisora y que el certificado esté disponible en la estación de administración que esté accediendo al iDRAC6. El valor **Ruta de acceso del archivo** muestra la ruta de acceso del archivo del certificado que se va a cargar. Si elige no buscar el certificado, introduzca la ruta de acceso del archivo, incluida la ruta de acceso completa y el nombre y la extensión del archivo completos.
Certificado de CA de Active Directory actual	Muestra el certificado de CA de Active Directory que se cargó al iDRAC6.
Paso 2 de 4 Configuración y administración de Active Directory	
Active Directory activado	Seleccione esta opción si desea activar Active Directory.

Tabla 5-19. Valores de configuración de Active Directory *(continuación)*

Valor	Descripción
Activar inicio de sesión mediante tarjeta inteligente	Seleccione esta opción para activar el inicio de sesión mediante tarjeta inteligente. Se le pedirá el inicio de sesión mediante tarjeta inteligente durante cualquier intento subsiguiente de inicio de sesión mediante la interfaz gráfica de usuario. **NOTA:** Las funciones de autentificación de dos factores (TFA) con tarjeta inteligente e inicio de sesión único sólo se admiten en los sistemas operativos Microsoft Windows con Internet Explorer. Además, los servicios de Terminal Server (escritorio remoto) en Windows XP no son compatibles con la tarjeta inteligente. Sin embargo, Windows Vista admite esta utilización.
Activar inicio de sesión único	Seleccione esta opción si desea iniciar sesión en el iDRAC6 sin necesidad de introducir credenciales de autentificación de usuario de dominio, por ejemplo, nombre de usuario y contraseña. Si activa el inicio de sesión único (SSO) y luego se desconecta, puede volver a iniciar sesión mediante SSO. Si ya inició sesión a través de SSO y luego se desconectó, o si falló el SSO, se mostrará la página web normal de inicio de sesión. **NOTA:** Activar el inicio de sesión mediante tarjeta inteligente **o** el inicio de sesión único no desactiva ninguna interfaz fuera de banda de línea de comandos, incluidos SSH, Telnet, RACADM remoto e IPMI en la LAN. **NOTA:** En esta versión, la función de autenticación de dos factores (TFA) con tarjeta inteligente no puede utilizarse si Active Directory está configurado para el esquema extendido. La función de inicio de sesión único (SSO) se admite tanto para el esquema estándar como para el esquema extendido.

Tabla 5-19. Valores de configuración de Active Directory *(continuación)*

Valor	Descripción
Nombre de dominio del usuario	Introduzca las anotaciones del nombre de dominio del usuario. Si esta opción está configurada, en la página de inicio de sesión aparecerá una lista de nombres de dominios de usuarios como menú desplegable. Si no está configurada, los usuarios de Active Directory podrán iniciar sesión al introducir el nombre de usuario con el formato nombre_de_usuario@nombre_de_dominio o nombre_de_dominio\nombre_de_usuario. **Agregar**: añade una nueva entrada de nombre de dominio de usuario a la lista. **Editar**: modifica una entrada existente de nombre de dominio de usuario. **Eliminar**: elimina una entrada de la lista de nombre de dominio de usuario.
Tiempo de espera	Introduzca el tiempo máximo (en segundos) de espera para que terminen las consultas a Active Directory.
Buscar controladores de dominio con DNS	Seleccione la opción **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory de una búsqueda en el DNS. Al seleccionar esta opción, se ignoran las direcciones 1-3 del servidor del controlador de dominio. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. De lo contrario, seleccione la opción **Especificar un dominio** e introduzca el nombre de dominio para usar en la búsqueda en el DNS. iDRAC6 tratará de conectarse a cada una de las direcciones (las primeras 4 direcciones que encuentre la búsqueda de DNS), una a la vez, hasta establecer una conexión satisfactoriamente. Si se selecciona el **esquema extendido**, los controladores de dominio se encuentran donde están ubicados el objeto dispositivo iDRAC6 y los objetos de asociación. Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.

Tabla 5-19. Valores de configuración de Active Directory *(continuación)*

Valor	Descripción
Especificar direcciones del controlador de dominio	Seleccione la opción **Especificar direcciones del controlador de dominio** para que el iDRAC6 pueda utilizar las direcciones especificadas del servidor del controlador de dominio de Active Directory. Al seleccionar esta opción, no se realiza la búsqueda en DNS. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Al seleccionar la opción **Especificar direcciones del controlador de dominio**, es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. Si la opción **esquema estándar** está seleccionada, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones. Si la opción **Esquema extendido** está seleccionada, las direcciones representan los controladores de dominio donde se encuentran el objeto dispositivo iDRAC6 y los objetos de asociación.
Paso 3 de 4 Configuración y administración de Active Directory	
Selección de esquema ampliado	Seleccione esta opción si desea utilizar el esquema ampliado con Active Directory. Haga clic en **Siguiente** para mostrar la página **Paso 4 de 4 Configuración y administración de Active Directory**. **Nombre del iDRAC6**: especifica el nombre que identifica de manera exclusiva el iDRAC6 en Active Directory. De manera predeterminada, este valor es NULO. **Nombre de dominio del iDRAC6**: El nombre de DNS (cadena) del dominio donde reside el objeto del iDRAC de Active Directory. De manera predeterminada, este valor es NULO. Estos valores sólo aparecen si el iDRAC6 fue configurado para utilizarse con el esquema ampliado de Active Directory.

Tabla 5-19. Valores de configuración de Active Directory *(continuación)*

Valor	Descripción
Selección de esquema estándar	Seleccione esta opción si desea utilizar el esquema estándar con Active Directory. Haga clic en **Siguiente** para mostrar la página **Paso 4a de 4 de Active Directory**. Seleccione la opción **Buscar servidores de catálogo global con DNS** e introduzca el **Nombre del dominio raíz** para usarlo en una búsqueda de DNS a fin de obtener los servidores de catálogo global de Active Directory. Al seleccionar esta opción, se ignoran las **direcciones 1-3 del servidor del catálogo global**. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión satisfactoria El servidor de catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. Seleccione la opción **Especificar direcciones del servidor del catálogo global** y escriba la dirección IP o el nombre de dominio completo (FQDN) del/de los servidor(es) del catálogo global. Al seleccionar esta opción, no se realiza la búsqueda en DNS. Al menos una de las tres direcciones debe estar configurada. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. El servidor de catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios. **Grupos de funciones:** especifica la lista de grupos de función asociados al iDRAC6. **Nombre de grupo:** especifica el nombre que identifica el grupo de funciones en Active Directory relacionado con el iDRAC6. **Dominio del grupo:** especifica el tipo de dominio del grupo donde reside el grupo de funciones. **Privilegios de grupo de funciones:** especifica el nivel de privilegio del grupo. (ver Tabla 5-20). Estos valores sólo aparecerán si el iDRAC6 fue configurado para utilizarse con el esquema estándar de Active Directory.

Tabla 5-20. Privilegios del grupo de funciones

Valor	Descripción
Nivel de privilegio del grupo de funciones	Especifica el privilegio máximo del usuario de iDRAC6 como uno de los siguientes: **Administrador**, **Usuario avanzado**, **Usuario invitado**, **Ninguno** o **Personalizado**. Ver Tabla 5-21 para ver los permisos del **Grupo de funciones.**
Iniciar sesión en el iDRAC6	Permite que el grupo inicie sesión en el iDRAC6.
Configurar el iDRAC6	Da permiso al grupo para configurar el iDRAC6.
Configurar usuarios	Da permiso al grupo para configurar usuarios.
Borrar registros	Da permiso al grupo para borrar registros.
Ejecutar comandos de control del servidor	Da permiso al grupo para ejecutar comandos de control del servidor.
Acceder a la consola virtual	Permite que el grupo tenga acceso a la consola virtual.
Acceder a los medios virtuales	Permite que el grupo tenga acceso a los soportes virtuales.
Probar alertas	Permite al grupo enviar alertas de prueba (mensajes de correo electrónico y capturas de sucesos de plataforma) a un usuario específico.
Ejecutar comandos de diagnóstico	Da permiso al grupo para ejecutar comandos de diagnóstico.

Tabla 5-21. Permisos del grupo de funciones

Propiedad	Descripción
Administrador	Iniciar sesión en el iDRAC6, Configurar el iDRAC6, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico

Tabla 5-21. Permisos del grupo de funciones *(continuación)*

Propiedad	Descripción
Usuario avanzado	Iniciar sesión en el iDRAC6, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas
Usuario invitado	Iniciar sesión en el iDRAC6
Custom (Personalizar)	Selecciona cualquier combinación de los permisos siguientes: Iniciar sesión en el iDRAC6, Configurar el iDRAC6, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico
None	Sin permisos asignados

Cómo ver un certificado de CA de Active Directory

En la pantalla de resumen de **Active Directory**, haga clic en **Configurar Active Directory**. Se muestra la sección **Certificado de CA de Active Directory actual**. Vea la Tabla 5-22.

Tabla 5-22. Información del certificado de CA de Active Directory

Campo	Descripción
Serial Number (Número de serie)	El número de serie del certificado.
Información del titular	Los atributos del certificado introducidos por el titular.
Información del emisor	Los atributos del certificado generados por el emisor.
Válido desde	La fecha de emisión del certificado.
Válido hasta	La fecha de expiración del certificado.

Activación o desactivación del acceso a la configuración local

NOTA: La configuración predeterminada para el acceso a la configuración local es Activado.

Activación del acceso a la configuración local

1. Haga clic en **Sistema**→ **Configuración de iDRAC**→ **Red/Seguridad**→ **Servicios**.
2. En **Configuración local**, haga clic para **deseleccionar** la casilla **Desactivar actualizaciones de Configuración de USUARIO iDRAC6 local** para activar el acceso.
3. Haga clic en **Aplicar**.

Desactivación del acceso a la configuración local

1. Haga clic en **Sistema**→ **Configuración de iDRAC**→ **Red/Seguridad**→ **Servicios**.
2. En **Configuración local**, haga clic para seleccionar la casilla **Desactivar actualizaciones de Configuración de USUARIO iDRAC6 local** para desactivar el acceso.
3. Haga clic en **Aplicar**.

Configuración de los servicios del iDRAC6

NOTA: Para modificar esta configuración, debe contar con permiso para Configurar el iDRAC6.

NOTA: Cuando se aplican cambios en los servicios, los cambios surten efecto inmediatamente. Las conexiones existentes pueden ser terminadas sin aviso.

NOTA: Existe un problema conocido con el cliente Telnet suministrado con Microsoft Windows. Utilice otro cliente Telnet como HyperTerminal o PuTTY.

1. Haga cic en **Sistema**→ **Configuración de iDRAC**→ ficha **Red/Seguridad**.
2. Haga clic en **Servicios** para abrir la pantalla de configuración **Servicios**.
3. Configure los servicios siguientes según sea necesario:
   - Web Server: ver Tabla 5-23 para ver la configuración del Web Server

- SSH: ver Tabla 5-24 para ver la configuración de SSH
- Telnet: ver Tabla 5-25 para ver la configuración de Telnet
- Agente SNMP: ver Tabla 5-26 para obtener información acerca de la configuración del agente SNMP
- Agente de recuperación automatizada del sistema: ver Tabla 5-27 para ver la configuración del agente de recuperación automatizada del sistema

4 Haga clic en **Aplicar**.

Tabla 5-23. Configuración del servidor Web

Valor	Descripción
Enabled	Activa o desactiva Web Server del iDRAC6. Cuando está **seleccionado**, indica que Web Server está activado. El valor predeterminado es **seleccionado**.
N.º máx. de sesiones	El número máximo de sesiones del servidor web simultáneas que se permite para este sistema. Este campo no se puede editar. Puede haber 4 sesiones simultáneas de Web Server.
Sesiones activas	El número de sesiones actuales en el sistema, menor o igual al **Máx. de sesiones**. Este campo no se puede editar.
Tiempo de espera	El tiempo, en segundos, permitido para que la conexión permanezca inactiva. La sesión se cierra cuando se alcanza el tiempo de espera. Los cambios en el valor de tiempo de espera surtirán efecto inmediatamente y restablecerán el servidor Web. El rango de tiempo de espera es de 60 a 10800 segundos. El valor predeterminado es de **1800** segundos.
Número de puerto de HTTP	El puerto en el que el iDRAC6 espera una conexión de explorador. El valor predeterminado es **80**.
Número de puerto HTTPS	El puerto en el que el iDRAC6 espera una conexión de explorador segura. El valor predeterminado es **443**.

Tabla 5-24. Configuración de SSH

Valor	Descripción
Activado	Activa o desactiva el SSH. Cuando está **seleccionada**, la casilla de verificación indica que SSH está activado.
N.º máx. de sesiones	El número máximo de sesiones SSH simultáneas que se permite para este sistema. Se admiten 4 sesiones SSH simultáneas. No puede editar este campo.
Sesiones activas	El número de sesiones actuales en el sistema. No puede editar este campo.
Tiempo de espera	El tiempo de espera en inactividad de Secure Shell, expresado en segundos. El rango de tiempo de espera es de 60 a 10800 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **1800**.
Port Number (Número de puerto)	El puerto en el que el iDRAC6 espera una conexión SSH. El valor predeterminado es **22**.

Tabla 5-25. Configuración de Telnet

Valor	Descripción
Activado	Activa o desactiva Telnet. Cuando está **seleccionado**, Telnet está activado. El valor predeterminado es **deseleccionado**.
N.º máx. de sesiones	El número máximo de sesiones simultáneas Telnet que se permite para este sistema. Se admiten 4 sesiones Telnet simultáneas. No puede editar este campo.
Sesiones activas	El número actual de sesiones Telnet en el sistema. No puede editar este campo.
Tiempo de espera	El tiempo de espera en inactividad de Telnet, en segundos. El rango de tiempo de espera es de 60 a 10800 segundos. Introduzca 0 segundos para desactivar la función de tiempo de espera. El valor predeterminado es **1800**.
Port Number (Número de puerto)	El puerto en el que el iDRAC6 espera una conexión Telnet. El valor predeterminado es **23**.

Tabla 5-26. Configuraciones de SNMP

Valor	Descripción
Activado	Activa/desactiva SNMP. Cuando se selecciona, SNMP está activado.
Nombre de comunidad SNMP	Introduzca el nombre de la comunidad de SNMP. El valor predeterminado es **público**.

Tabla 5-27. Agente de recuperación automática del sistema

Valor	Descripción
Activado	Activa el agente de recuperación automática del sistema.

Actualización del firmware de iDRAC6

NOTA: Si el firmware del iDRAC6 se daña, como puede suceder cuando la actualización del firmware del iDRAC6 se interrumpe antes de terminar, puede recuperar el iDRAC6 por medio del CMC. Consulte la *Guía del usuario del firmware del CMC* para obtener instrucciones.

NOTA: De manera predeterminada, la actualización del firmware conserva la configuración actual del iDRAC6. Durante el proceso de actualización, tiene la opción de restablecer la configuración predeterminada de fábrica del iDRAC6. Si establece la configuración predeterminada de fábrica, el acceso a la red externa se desactivará cuando la actualización termine. Debe activar y configurar la red por medio de la utilidad de configuración del iDRAC6 o la interfaz web del CMC.

1 Inicie la interfaz web del iDRAC6.

2 Haga clic en **Sistema**→ **Configuración de iDRAC**→ ficha **Actualizar**.

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

NOTA: Para actualizar el firmware, el iDRAC6 debe estar en el modo de actualización. Cuando se encuentre en este modo, el iDRAC6 se restablecerá automáticamente, aun cuando usted cancele el proceso de actualización.

3 En la sección **Cargar**, haga clic en **Examinar** y seleccione la imagen del firmware.

El nombre predeterminado de la imagen del firmware es **firmimg.imc**.

4 Haga clic en **Cargar**. El archivo se cargará en el iDRAC6. This may take several minutes to complete.

5 En la página **Cargar (paso 2 de 3)**, verá los resultados de la validación realizada sobre el archivo de imagen que se cargó.

- Cuando el archivo de imagen se cargue correctamente y pase todas las revisiones de verificación, aparecerá un mensaje que indicará que la imagen del firmware ha sido verificada.
- Si la imagen no se cargó correctamente, ni pasó las revisiones de verificación, restablezca el iDRAC6, cierre le sesión actual y luego intente actualizar nuevamente.

NOTA: Si tras la finalización de una actualización de firmware, selecciona la casilla de verificación **Conservar configuración**, el iDRAC6 se restablecerá a su configuración predeterminada. En la configuración predeterminada, la LAN está desactivada. Usted no podrá iniciar sesión en la interfaz web del iDRAC6. Deberá reconfigurar los valores de la LAN por medio de la interfaz web del CMC mediante la utilidad de configuración del iDRAC6 durante la POST del BIOS.

6 De manera predeterminada, la casilla de verificación **Conservar configuración** está seleccionada para conservar los valores actuales en el iDRAC6 después de una actualización. Si no desea conservar los valores, deseleccione la casilla de verificación de marcación **Conservar configuración**.

7 Haga clic en **Comenzar la actualización** para iniciar el proceso de actualización. No interrumpa el proceso de actualización.

8 En la ventana **Actualización (paso 3 de 3)**, verá el estado de la actualización. El progreso de la operación de actualización de firmware, expresado en porcentaje, aparecerá en la columna **Progreso**.

9 Una vez que la actualización del firmware concluya, la ventana **Actualización (paso 3 de 3)** se actualizará con el resultado y el iDRAC6 se restablecerá automáticamente. Para continuar accediendo al iDRAC6 a través de la interfaz web, cierre la ventana actual del explorador y vuelva a conectarse al iDRAC6 utilizando una ventana nueva de explorador.

Actualización del firmware del iDRAC6 por medio del CMC

Normalmente, el firmware del iDRAC6 se actualiza por medio de las utilidades de iDRAC6, por ejemplo, la interfaz web del iDRAC6 o los paquetes de actualización específicos del sistema operativo que descargó de **support.dell.com**.

Puede utilizar la interfaz web o RACADM del CMC para actualizar el firmware del iDRAC6. Esta función está disponible cuando el firmware del iDRAC6 está en modo Normal y cuando está dañado.

NOTA: Consulte la *Guía del usuario de firmware de Chassis Management Controller* para obtener instrucciones acerca del uso de la interfaz web del CMC.

Para actualizar el firmware del iDRAC6, realice los pasos a continuación:

1. Descargue el firmware más reciente del iDRAC6 a la estación de administración en **support.dell.com**.
2. Inicie sesión en la interfaz web del CMC.
3. Haga clic en **Descripción general del chasis** en el árbol del sistema.
4. Haga clic en la ficha **Actualizar**. Se muestra la pantalla **Actualización del firmware**.
5. En la sección **Firmware de Entreprise del iDRAC6→** columna **Actualizar destinos**, seleccione los iDRAC6 a actualizar.
6. Haga clic en **Aplicar la actualización Entreprise del iDRAC6**.
7. Haga clic en **Examinar**, busque la imagen del firmware del iDRAC6 que descargó y haga clic en **Abrir**.
8. Haga clic en **Iniciar actualización del firmware**.

Después de que el archivo de imagen del firmware haya sido cargado en el CMC, el iDRAC6 se actualizará con la imagen.

NOTA: Cuando se actualiza iDRAC mediante la interfaz de web de CMC, siempre se conservará la configuración.

Reversión del firmware del iDRAC6

iDRAC6 es capaz de mantener dos imágenes de firmware simultáneamente. Puede optar por iniciar desde la imagen de firmware de su elección o revertir el firmware a dicha imagen.

1. Abra la interfaz web del iDRAC6 e inicie sesión en el sistema remoto.

2 Haga clic en **Sistema→ Xonfiguración de iDRAC→** ficha **Actualizar**.

3 Haga clic en **Revertir**. Las versiones de firmware actuales y anteriores se muestran en la página **Revertir (paso 2 de 3)**.

4 Haga clic en **Siguiente** para iniciar el proceso de reversión de firmware.

En la página **Revertir (paso 3 de 3)**, se mostrará el estado de la operación de reversión. Una vez que se haya completado correctamente, se muestra que el proceso se completó satisfactoriamente.

Si la reversión del firmware es correcta, el iDRAC6 se restablecerá automáticamente. Para continuar trabajando con el iDRAC6 a través de la interfaz web, cierre la ventana actual del explorador y vuelva a conectarse al iDRAC6 utilizando una ventana nueva de explorador. Si se detecta un error, aparece el mensaje de error correspondiente.

NOTA: La función **Conservar configuración** no funciona si desea revertir el firmware del iDRAC6 de la versión 2.2 a la versión 2.1.

6

Uso del servicio de directorio de iDRAC6

Un servicio de directorio mantiene una base de datos común para almacenar información sobre los usuarios, equipos, impresoras, etc. de una red. Si la empresa utiliza el software Active Directory de Microsoft o el servicio de directorio LDAP, puede configurarlo para que proporcione acceso al iDRAC6, lo que le permite agregar y controlar los privilegios de usuario del iDRAC6 de los usuarios existentes del servicio de directorio.

Uso del iDRAC6 con Microsoft Active Directory

NOTA: El uso de Active Directory para reconocer usuarios del iDRAC6 se admite en los sistemas operativos Microsoft Windows 2000, Windows Server 2003 y Windows Server 2008.

Puede configurar la autentificación de usuario mediante Microsoft Active Directory para iniciar sesión en el iDRAC6. También puede proporcionar autoridad basada en la función, lo que activa al administrador para configurar privilegios específicos para cada usuario. Para obtener más información, consulte las secciones subsiguientes.

La Tabla 6-1 muestra los privilegios de usuario de Active Directory del iDRAC6.

Tabla 6-1. Privilegios de usuario del iDRAC6

Privilegio	Descripción
Iniciar sesión en el iDRAC6	Permite al usuario iniciar sesión en el iDRAC6.
Configurar el iDRAC6	Permite al usuario configurar iDRAC6.
Configurar usuarios	Permite al usuario otorgar acceso al sistema a usuarios específicos.
Borrar registros	Permite al usuario borrar los registros del iDRAC6.
Ejecutar comandos de control del servidor	Permite al usuario ejecutar comandos de RACADM.
Acceder a la consola virtual	Permite al usuario ejecutar la consola virtual.

Tabla 6-1. Privilegios de usuario del iDRAC6 *(continuación)*

Privilegio	Descripción
Acceder a los medios virtuales	Permite al usuario ejecutar y usar los medios virtuales.
Probar alertas	Permite al usuario enviar alertas de prueba (por correo electrónico y PET) a un usuario específico.
Ejecutar comandos de diagnóstico	Permite al usuario ejecutar comandos de diagnóstico.

Puede utilizar Active Directory para iniciar sesión en el iDRAC6 mediante uno de los siguientes métodos:

- Interfaz de web
- RACADM local
- SSH o consola Telnet para la interfaz de línea de comandos de SM-CLP

La sintaxis de inicio de sesión es la misma para los tres métodos:

<nombre_de_usuario@dominio>

o

*<dominio>**<nombre_de_usuario>* o
<dominio>/*<nombre_de_usuario>*

donde *nombre_de_usuario* es una cadena ASCII de 1 a 256 bytes.

No se permite usar espacios en blanco ni caracteres especiales (como \, / ó @) en el nombre de usuario ni en el nombre de dominio.

NOTA: No se pueden especificar nombres de dominio NetBIOS, como "*América*", porque estos nombres no se pueden resolver.

Si inicia sesión en la interfaz web y ha configurado dominios de usuario, aparecerá en pantalla un menú desplegable de todos los dominios de usuario para que seleccione el deseado. Si selecciona un dominio de usuario del menú desplegable, sólo debe introducir el nombre de usuario. Aun si selecciona **Este iDRAC**, podrá iniciar sesión como usuario de Active Directory si utiliza la sintaxis de inicio de sesión descrita anteriormente en "Uso del iDRAC6 con Microsoft Active Directory" en la página 133.

Prerrequisitos para activar la autentificación de Active Directory para iDRAC6

Para utilizar la función de autentificación de Active Directory del iDRAC6, debe haber implementado una infraestructura de Active Directory. Consulte el sitio web de Microsoft para obtener información sobre cómo configurar una infraestructura de Active Directory si aún no tiene una.

El iDRAC6 utiliza el mecanismo estándar de infraestructura de clave pública (PKI) para autentificar de manera segura en Active Directory; por lo tanto, necesitará también una PKI integrada en la infraestructura de Active Directory.

Consulte el sitio web de Microsoft para obtener más información sobre la configuración de PKI.

Para autentificar correctamente todos los controladores de dominio, también necesitará activar la capa de sockets seguros (SSL) en todos los controladores de dominio a los que se conecte el iDRAC6. Ver "Activación de SSL en un controlador de dominio" en la página 135 para obtener información más específica.

Activación de SSL en un controlador de dominio

Cuando el iDRAC6 autentifica usuarios con un controlador de dominio de Active Directory, inicia una sesión SSL con el controlador de dominio. En este momento, el controlador de dominio debe publicar un certificado firmado por la autoridad de certificados (CA), cuyo certificado raíz se carga en el iDRAC6. En otras palabras, para que el iDRAC6 pueda autentificarse en *cualquier* controlador de dominio (sin importar si es el controlador de dominio raíz o secundario), el controlador de dominio debe tener un certificado activado para SSL firmado por la CA del dominio.

Si va a usar la CA de certificados raíz de Microsoft para asignar *automáticamente* todos los controladores de dominio a un certificado SSL, realice los pasos siguientes para activar el SSL en cada controlador de dominio:

1. Active SSL en cada uno de los controladores de dominio mediante la instalación del certificado SSL para cada controlador.
   a. Haga clic en **Inicio→ Herramientas administrativas→ Política de seguridad del dominio**.

b Amplíe la carpeta **Directivas de claves públicas**, haga clic con el botón derecho del mouse en **Configuración de la solicitud de certificados automática** y haga clic en **Solicitud de certificados automática**.

c En el **Asistente para instalación de solicitud de certificados automática**, haga clic en **Siguiente** y seleccione **Controlador de dominio**.

d Haga clic en **Siguiente** y luego en **Terminar**.

Exportación del certificado de CA del controlador de dominio raíz a iDRAC6

NOTA: Si el sistema ejecuta Windows 2000, los siguientes pasos pueden variar.

NOTA: Si está utilizando una autoridad de certificación independiente, los siguientes pasos pueden presentar diferencias.

1 Localice el controlador de dominio que ejecuta el servicio de CA de Microsoft Enterprise.

2 Haga clic en **Start** (Inicio)→ **Run** (Ejecutar).

3 En el campo **Ejecutar**, introduzca `mmc` y haga clic en **Aceptar**.

4 En la ventana **Consola 1** (MMC), haga clic en **Archivo** (o **Consola** en sistemas Windows 2000) y seleccione **Agregar/quitar complemento**.

5 En la ventana **Agregar/quitar complemento**, haga clic en **Agregar**.

6 En la ventana **Complemento independiente**, seleccione **Certificados** y haga clic en **Agregar**.

7 Seleccione la cuenta **Equipo** y haga clic en **Siguiente**.

8 Seleccione **Equipo local** y haga clic en **Terminar**.

9 Haga clic en **OK** (Aceptar).

10 En la ventana **Consola 1**, amplíe la carpeta **Certificados**, amplíe la carpeta **Personal** y haga clic en la carpeta **Certificados**.

11 Ubique y haga clic con el botón derecho del mouse en el certificado de CA raíz, seleccione **Todas las tareas** y haga clic en **Exportar...**

12 En el **Asistente de exportación de certificados**, haga clic en **Siguiente** y seleccione **No exportar la clave privada**.

13 Haga clic en **Siguiente** y seleccione **Codificado en base 64 X.509 (.cer)** como el formato.

14 Haga clic en **Siguiente** y guarde el certificado en un directorio del sistema.

15 Cargue el certificado que guardó en el paso paso 14 en el iDRAC6.

Para cargar el certificado por medio de RACADM, ver "Configuración de Active Directory con esquema estándar vía RACADM" en la página 166.

Para cargar el certificado desde la interfaz web, ver "Configuración de Active Directory con esquema estándar mediante la interfaz web del iDRAC6" en la página 162.

Importar el certificado SSL de firmware del iDRAC6

NOTA: Si el servidor de Active Directory está configurado para autentificar el cliente durante la fase de inicialización de una sesión SSL, deberá cargar también el certificado del servidor del iDRAC6 en el controlador de dominio de Active Directory. Este paso adicional no es necesario si Active Directory no realiza la autentificación de cliente durante la fase de inicialización de una sesión SSL.

NOTA: Si el sistema ejecuta Windows 2000, los siguientes pasos pueden variar.

NOTA: Si el certificado SSL de firmware del iDRAC6 está firmado por una entidad emisora reconocida y dicho certificado ya se encuentra en la lista de certificados de una entidad emisora raíz de confianza del controlador de dominio, no es necesario realizar los pasos detallados en esta sección.

El certificado SSL del iDRAC6 es el certificado idéntico que se utiliza para el Web Server del iDRAC6. Todos los controladores del iDRAC6 se envían con un certificado predeterminado firmado automáticamente.

Para importar el certificado SSL del firmware iDRAC6 en todas las listas de certificado seguras de la controladora de dominio:

1 Para descargar el certificado SSL del iDRAC6, ejecute el siguiente comando RACADM:

```
racadm sslcertdownload -t 0x1 -f <certificado SSL del RAC>
```

2 En el controlador del dominio, abra una ventana **Consola de MMC** y seleccione **Certificados→ Autoridades de certificación de raíz confiables**.

3 Haga clic con el botón derecho del mouse en **Certificados**, seleccione **Todas las tareas** y haga clic en **Importar**.

4 Haga clic en **Siguiente** y desplácese al archivo de certificado SSL.

5 Instale el certificado SSL del iDRAC6 en la lista de **Entidades emisoras raíz de confianza** de cada controlador de dominio.

Si ha instalado su propio certificado, asegúrese que la CA que firma el certificado esté en la lista **Autoridades de certificación de raíz confiables**. Si la autoridad no está en la lista, debe instalarla en todos los controladores de dominio.

6 Haga clic en **Siguiente** y especifique si desea que Windows seleccione automáticamente el almacén de certificados basándose en el tipo de certificado, o examine hasta encontrar un almacén de su elección.

7 Haga clic en **Terminar** y luego en **Aceptar**.

Mecanismos de autentificación compatibles de Active Directory

Puede utilizar Active Directory para definir el acceso de los usuarios en el iDRAC6 mediante dos métodos: por medio de la solución de *esquema extendido* que Dell ha personalizado para agregar objetos de Active Directory definidos por Dell. También se puede usar la solución de *esquema estándar*, que utiliza únicamente objetos de grupo de Active Directory. Consulte las siguientes secciones para obtener más información sobre estas soluciones.

Cuando se usa Active Directory para configurar el acceso al iDRAC6, se debe elegir la solución de esquema extendido o de esquema estándar.

Las ventajas de usar la solución de esquema extendido son:

- Todos los objetos de control de acceso se mantienen en Active Directory.
- Se proporciona máxima flexibilidad para configurar el acceso de los usuarios en diferentes tarjetas del iDRAC6 con distintos niveles de privilegios.

La ventaja de utilizar la solución de esquema estándar radica en que no se requiere una extensión del esquema, ya que la configuración predeterminada del esquema de Active Directory que proporciona Microsoft proporciona todas las clases de objetos necesarias.

Generalidades del esquema ampliado de Active Directory

Para utilizar la solución de esquema extendido, es necesario una extensión del esquema de Active Directory, según se describe en la siguiente sección.

Extensiones de esquema de Active Directory

Los datos de Active Directory son una base de datos distribuida de atributos y clases. El esquema de Active Directory incluye las reglas que determinan el tipo de datos que se pueden agregar o incluir en la base de datos. La clase de usuario es un ejemplo de una clase que se almacena en la base de datos. Algunos ejemplos de atributos de clase de usuario incluyen el nombre y el apellido del usuario, el número telefónico, etc. Las empresas pueden extender la base de datos de Active Directory al agregar sus propios atributos y clases exclusivos para solucionar las necesidades específicas del entorno. Dell ha extendido el esquema para incluir los cambios necesarios para admitir la autentificación y autorización de administración remota.

Cada atributo o clase que se agrega a un esquema existente de Active Directory debe ser definido con una identificación única. Para que las identificaciones se mantengan exclusivas en toda la industria, Microsoft conserva una base de datos de Identificadores de Objeto de Active Directory (OID) para que cuando las compañías agregan extensiones al esquema, se pueda garantizar que serán exclusivas y no entrarán en conflicto una con otra. Para extender el esquema en Active Directory de Microsoft, Dell recibió OID exclusivos, extensiones de nombre exclusivas e identificaciones de atributo vinculadas exclusivamente para las clases y los atributos agregados al servicio de directorio.

- La extensión de Dell es: `dell`
- El OID base de Dell es: `1.2.840.113556.1.8000.1280`
- El rango del LinkID de RAC es: `12070 a 12079`

Descripción de las extensiones de esquema del iDRAC6

Para proporcionar la mayor flexibilidad en la multitud de entornos de cliente, Dell proporciona un grupo de propiedades que el usuario puede configurar según los resultados deseados. Dell ha extendido el esquema para incluir propiedades de asociación, dispositivo y privilegio. La propiedad de asociación se utiliza para vincular a los usuarios o los grupos que tienen un conjunto específico de privilegios para uno o varios dispositivos iDRAC6. Este modelo proporciona máxima flexibilidad al administrador con respecto a las diferentes combinaciones de usuarios, privilegios del iDRAC6 y dispositivos iDRAC6 en la red sin aumentar demasiado la complejidad.

Descripción general de los objetos de Active Directory

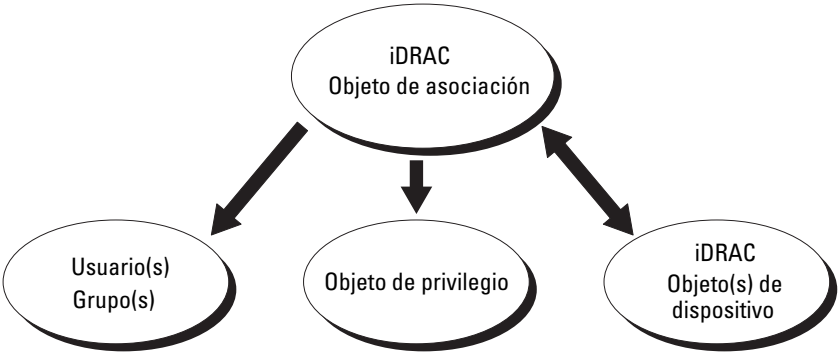
Por cada uno de los dispositivos iDRAC6 físicos de la red que desee integrar con Active Directory para autentificación y autorización, cree al menos un objeto de asociación y un objeto de dispositivo iDRAC6. Puede crear varios objetos de asociación y cada uno de ellos puede vincularse a cuantos usuarios, grupos de usuarios u objetos de dispositivo iDRAC6 sean necesarios. Los usuarios y los grupos de usuarios del iDRAC6 pueden ser miembros de cualquier dominio de la empresa.

Sin embargo, cada objeto de asociación puede vincularse (o es posible que vincule usuarios, grupos de usuarios u objetos de dispositivo iDRAC6) sólo a un objeto de privilegio. Este ejemplo permite que el administrador controle los privilegios de cada usuario en dispositivos iDRAC6 específicos.

El objeto del dispositivo iDRAC6 es el vínculo al firmware del iDRAC6 para consultar Active Directory para autentificación y autorización. Cuando se agrega el iDRAC6 a la red, el administrador debe configurar el iDRAC6 y su objeto de dispositivo con su nombre de Active Directory para que los usuarios puedan realizar la autentificación y la autorización con Active Directory. Además, el administrador debe agregar iDRAC6 a un objeto de asociación por lo menos para que los usuarios se puedan autentificar.

La Ilustración 6-1 muestra que el objeto de asociación proporciona la conexión necesaria para todas las autentificaciones y autorizaciones.

Ilustración 6-1. Configuración típica de los objetos de Active Directory



Se pueden crear tantos objetos de asociación como sean necesarios. Sin embargo, debe crear al menos un objeto de asociación y debe tener un objeto de dispositivo iDRAC6 por cada dispositivo iDRAC6 de la red que desea integrar con Active Directory para autentificación y autorización con iDRAC6.

El objeto de asociación permite toda cantidad de usuarios o grupos, así como de objetos de dispositivo iDRAC6. Sin embargo, el objeto de asociación solo incluye un objeto de privilegio por cada objeto de asociación. El objeto de asociación conecta a los *usuarios* con *privilegios* en los dispositivos iDRAC6.

La extensión de Dell al complemento MMC de ADUC sólo permite asociar el objeto de privilegio y los objetos del iDRAC6 del mismo dominio con el objeto de asociación. La extensión de Dell no permite que un grupo o un objeto iDRAC6 de otro dominio se agregue como miembro del producto del objeto de asociación.

Cuando se agregan grupos universales a partir de dominios separados, se debe crear un objeto de asociación con ámbito universal. Los objetos de asociación predeterminados creados por la utilidad Dell Schema Extender, son grupos locales de dominio y no funcionarán con grupos universales de otros dominios.

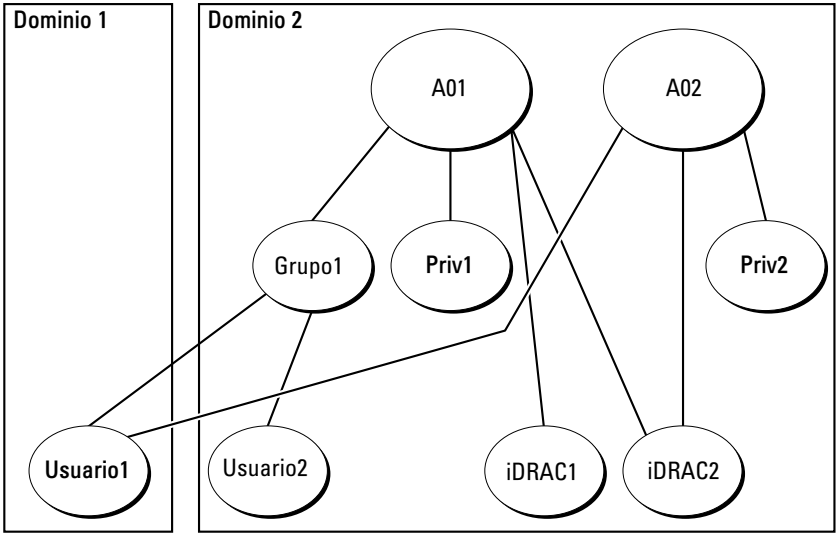
Los usuarios, los grupos de usuarios o los grupos de usuarios anidados de cualquier dominio pueden agregarse al objeto de asociación. Las soluciones de esquema extendido admiten todo tipo de grupos de usuarios o de grupo anidado de usuarios en varios dominios permitidos por Microsoft Active Directory.

Acumulación de privilegios con el esquema extendido

El mecanismo de autentificación del esquema extendido admite la acumulación de privilegios provenientes de distintos objetos de privilegio asociados al mismo usuario entre distintos objetos de asociación. En otras palabras, la autentificación del esquema extendido acumula privilegios para permitir al usuario el súper conjunto de todos los privilegios asignados que corresponden a los distintos objetos de privilegio asociados al mismo usuario.

La Ilustración 6-2 muestra un ejemplo de la acumulación de privilegios por medio del esquema extendido.

Ilustración 6-2. Acumulación de privilegios para un usuario



La figura muestra dos objetos de asociación: OA1 y OA2. El Usuario1 está asociado con el iDRAC2 por medio de ambos objetos de asociación. Por lo tanto, el Usuario1 ha acumulado privilegios que resultan de la combinación del conjunto de privilegios de los objetos Priv1 y Priv2 en el iDRAC2.

Por ejemplo, Priv1 tiene los privilegios: Inicio de sesión, Medios virtuales y Borrar registros; mientras que Priv2 tiene los privilegios: Inicio de sesión en iDRAC, Configurar el iDRAC y Probar alertas. Como resultado, el Usuario1 tiene ahora el conjunto de privilegios: Inicio de sesión en iDRAC, Medios virtuales, Borrar registros, Configurar el iDRAC y Alertas de prueba, que es el conjunto de privilegios combinados de Priv1 y Priv2.

La autentificación del esquema extendido acumula privilegios para permitir que el usuario tenga el conjunto máximo de privilegios según los privilegios asignados de los distintos objetos de privilegio asociados al mismo usuario.

En esta configuración, el Usuario1 tiene privilegios de Priv1 y Priv2 en iDRAC2. El Usuario1 tiene privilegios de Priv1 en iDRAC1 solamente. El Usuario2 tiene privilegios de Priv1 tanto en iDRAC1 como en iDRAC2. Además, esta ilustración muestra que el Usuario1 puede estar en un dominio diferente y ser miembro de un grupo.

Configuración de Active Directory con esquema extendido para acceder al iDRAC6

Antes de utilizar Active Directory para acceder al iDRAC6, debe configurar el software Active Directory y el iDRAC6. Para hacerlo, lleve a cabo los pasos siguientes en el orden indicado:

1. Amplíe el esquema de Active Directory (ver "Cómo extender el esquema de Active Directory" en la página 143).
2. Amplíe el complemento Usuarios y equipos de Active Directory (ver "Instalación de la extensión de Dell para el complemento Usuarios y equipos de Active Directory" en la página 150).
3. Agregue usuarios del iDRAC6 y sus privilegios a Active Directory (ver "Cómo agregar usuarios y privilegios del iDRAC6 a Active Directory" en la página 151).
4. Configure las propiedades de Active Directory del iDRAC6 por medio de la interfaz web del iDRAC6 o de RACADM (ver "Configuración de Active Directory de Microsoft con esquema extendido por medio de la interfaz web del iDRAC6" en la página 154 o "Configuración de Active Directory con esquema extendido por medio de RACADM" en la página 157).

Cómo extender el esquema de Active Directory

Importante: la extensión del esquema de este producto es distinta de la de generaciones anteriores de productos de Dell Remote Management. Deberá extender el nuevo esquema e instalar el nuevo **complemento Microsoft Management Console (MMC) de usuarios y equipos de Active Directory** en su directorio. El esquema anterior no funciona con este producto.

NOTA: La extensión del nuevo esquema y la instalación de la nueva extensión en el Complemento Usuarios y equipos de Active Directory no afectan las versiones anteriores del producto.

Puede encontrar el complemento MMC de usuarios y equipos de Active Directory y la extensión del esquema en el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management). Para obtener información sobre la instalación, ver "Instalación de la extensión de Dell para el complemento Usuarios y equipos de Active Directory" en la página 150. Para obtener detalles adicionales acerca de la extensión del esquema para iDRAC6 y la instalación del complemento MMC de Usuarios y equipos de Active Directory, consulte la *Dell OpenManage Installation and Security User's Guide* (Guía del usuario de instalación y seguridad de Dell OpenManage), disponible en **dell.com/support/manuals**.

NOTA: Cuando cree objetos de asociación o de dispositivo iDRAC6, seleccione **Dell Remote Management Object Advanced**.

La extensión del esquema de Active Directory agrega una unidad organizacional Dell, clases y atributos de esquema, así como privilegios y objetos de asociación de ejemplo al esquema de Active Directory. Antes de extender el esquema, compruebe que tiene privilegios de administrador de esquema en el propietario de la función de operación maestra simple y flexible (FSMO) del esquema en el bosque de dominio.

Puede extender el esquema por medio de uno de los siguientes métodos:

- Utilidad Dell Schema Extender
- Archivo de secuencia de comandos LDIF

Si utiliza el archivo de secuencia de comandos LDIF, la unidad organizacional de Dell no se agregará al esquema.

Los archivos LDIF y la utilidad Dell Schema Extender se encuentran en el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) en los siguientes directorios respectivamente:

- *Unidad de DVD*:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <*Unidad de DVD*>:**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Para usar los archivos LDIF, consulte las instrucciones en el archivo léame que se incluye en el directorio **LDIF_Files**. Para usar Dell Schema Extender para extender el esquema de Active Directory, ver "Uso de Dell Schema Extender" en la página 145.

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 asegurar que la utilidad Dell Schema Extender funcione correctamente, no modifique el nombre de este archivo.

1. En la pantalla de **Bienvenida**, haga clic en **Siguiente**.
2. Lea y comprenda la advertencia y haga clic en **Siguiente**.
3. Seleccione **Usar las credenciales de inicio de sesión actuales** o introduzca un nombre de usuario y una contraseña con derechos de administrador de esquema.
4. Haga clic en **Siguiente** para ejecutar Dell Schema Extender.
5. Haga clic en **Terminar**.

   El esquema ha sido extendido. Para verificar la extensión del esquema, utilice el complemento de esquema de Active Directory y MMC y verifique si existen los siguientes elementos:

   - Clases (ver Tabla 6-2 a Tabla 6-7)
   - Atributos (Tabla 6-8)

   Consulte la documentación de Microsoft para obtener información acerca de cómo utilizar el complemento de esquema de Active Directory y MMC.

Tabla 6-2. Definiciones de 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 6-3. Clase dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Descripción	Representa el dispositivo iDRAC6 de Dell. iDRAC6 debe estar configurado como delliDRACDevice en Active Directory. Esta configuración permite que el iDRAC6 envíe consultas de Protocolo ligero de acceso a directorios (LDAP) a Active Directory.
Tipo de clase	Clase estructural
Superclases	dellProduct
Atributos	**dellSchemaVersion** **dellRacType**

Tabla 6-4. Clase delliDRACAssociationObject

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Descripción	Representa el objeto de asociación de Dell. El objeto de asociación proporciona la conexión entre los usuarios y los dispositivos.
Tipo de clase	Clase estructural
Superclases	almacenamiento
Atributos	**dellProductMembers** **dellPrivilegeMember**

Tabla 6-5. Clase dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Descripción	Define los privilegios (Derechos de autorización) para iDRAC6
Tipo de clase	Clase auxiliar
Superclases	Ninguno

Tabla 6-5. Clase dellRAC4Privileges *(continuación)*

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Atributos	**dellIsLoginUser**
	dellIsCardConfigAdmin
	dellIsUserConfigAdmin
	dellIsLogClearAdmin
	dellIsServerResetUser
	dellIsConsoleRedirectUser
	dellIsVirtualMediaUser
	dellIsTestAlertUser
	dellIsDebugCommandAdmin

Tabla 6-6. 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
Superclases	Usuario
Atributos	**dellRAC4Privileges**

Tabla 6-7. Clase dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Descripción	La clase principal de la que se derivan todos los productos Dell.
Tipo de clase	Clase estructural
Superclases	Computadora
Atributos	**dellAssociationMembers**

Tabla 6-8. Lista de atributos agregados al esquema de Active Directory

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellPrivilegeMember Lista de los objetos dellPrivilege que pertenecen a este atributo.	1.2.840.113556.1.8000.1280.1.1.2.1 Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSO
dellProductMembers Lista de los objetos dellRacDevice y DelliDRACDevice que pertenecen a esta función. Este atributo es el vínculo de avance al vínculo de retroceso de dellAssociationMembers. Identificación de vínculo: 12070	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
dellIsLoginUser TRUE si el usuario tiene derechos de inicio de sesión en el dispositivo.	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
dellIsCardConfigAdmin TRUE si el usuario tiene derechos de configuración de tarjeta en el dispositivo.	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
dellIsUserConfigAdmin TRUE si el usuario tiene derechos de configuración de usuario en el dispositivo.	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
delIsLogClearAdmin TRUE si el usuario tiene derechos de borrado de registro en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.6 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsServerResetUser TRUE si el usuario tiene derechos de restablecimiento de servidor en el dispositivo.	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

Tabla 6-8. Lista de atributos agregados al esquema de Active Directory *(continuación)*

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellIsConsoleRedirectUser TRUE si el usuario tiene derechos de consola virtual en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.8 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsVirtualMediaUser TRUE si el usuario tiene derechos de medios virtuales en el dispositivo.	1.2.840.113556.1.8000.1280.1.1.2.9 Booleano (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	VERDADERO
dellIsTestAlertUser TRUE si el usuario tiene derechos de usuario de prueba de alertas en el dispositivo.	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
dellIsDebugCommandAdmin TRUE si el usuario tiene derechos de administrador de comandos de depuración en el dispositivo.	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
dellSchemaVersion La versión del esquema actual se usa para actualizar el esquema.	1.2.840.113556.1.8000.1280.1.1.2.12 Cadena en que se ignoran las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO
dellRacType Este atributo es el tipo de RAC actual para el objeto delliDRACDevice y el vínculo de retroceso al vínculo de avance de dellAssociationObjectMembers.	1.2.840.113556.1.8000.1280.1.1.2.13 Cadena en que se ignoran las mayúsculas (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	VERDADERO

Tabla 6-8. Lista de atributos agregados al esquema de Active Directory *(continuación)*

Nombre del atributo/Descripción	OID asignado/Identificador de objeto de sintaxis	Con un solo valor
dellAssociationMembers	1.2.840.113556.1.8000.1280.1.1.2.14	FALSO
Lista de dellAssociationObjectMembers que pertenecen a este producto. Este atributo es el enlace de retroceso al atributo vinculado dellProductMembers. Identificación de vínculo: 12071	Nombre distintivo (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	

Instalación de la extensión de Dell para el complemento Usuarios y equipos de Active Directory

Cuando se extiende el esquema en Active Directory, también debe extenderse el complemento Usuarios y equipos de Active Directory para que el administrador pueda administrar los dispositivos iDRAC6, los usuarios y los grupos de usuarios del iDRAC6, así como las asociaciones y privilegios del iDRAC6.

Cuando instala el software de administración de sistemas con el DVD **Dell Systems Management Tools and Documentation** (Documentación y herramientas de Dell Systems Management) puede extender el complemento si selecciona la opción *Complemento Usuarios y equipos de Active Directory* durante el procedimiento de instalación. Consulte la *Dell OpenManage Software Quick Installation Guide* (Guía de instalación rápida del software Dell OpenManage) para obtener más instrucciones sobre la instalación del software Systems Management. Para sistemas operativos de Windows de 64 bits, el programa de instalación del complemento se encuentra en :

<Unidad de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

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

Instalación de Administrator Pack

Debe instalar el paquete de administrador en cada sistema que administre los objetos iDRAC6 de Active Directory. Si no lo hace, no podrá ver el objeto iDRAC6 de Dell en el contenedor.

Ver "Cómo abrir el complemento Usuarios y equipos de Active Directory" en la página 151 para obtener más información.

Cómo abrir el complemento Usuarios y equipos de Active Directory

Para abrir el complemento de usuarios y equipos de Active Directory:

1. Si ya inició sesión en el controlador del dominio, haga clic en **Inicio Herramientas administrativas→ Usuarios y equipos de Active Directory**.

   Si no ha iniciado sesión en el controlador de dominio, el paquete de administrador de Microsoft correspondiente debe estar instalado en el sistema local. Para instalar el paquete de administrador, haga clic en **Inicio→ Ejecutar**, introduzca `MMC`, y presione **Intro**.

   Aparece la consola MMC.

2. En la ventana **Consola 1**, haga clic en **Archivo** (o en **Consola**, en los sistemas que ejecutan Windows 2000).
3. Haga clic en **Agregar o quitar complemento**.
4. Seleccione **Complemento de usuarios y equipos de Active Directory** y haga clic en **Agregar**.
5. Haga clic en **Cerrar** y luego en **Aceptar**.

Cómo agregar usuarios y privilegios del iDRAC6 a Active Directory

El Complemento Usuarios y equipos de Active Directory extendido por Dell permite agregar usuarios y privilegios del iDRAC6 mediante la creación de objetos de asociación y de privilegio del iDRAC6. Para agregar cada tipo de objeto, realice los pasos siguientes:

- Cree un objeto de dispositivo iDRAC6
- Cree un objeto de privilegio
- Cree un objeto de asociación
- Agregue los objetos a un objeto de asociación

Creación de un objeto del dispositivo iDRAC6

1. En la ventana **Raíz de consola** de MMC, haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el nuevo objeto. El nombre debe ser idéntico al nombre del iDRAC6 que va a escribir en el paso A de "Configuración de Active Directory de Microsoft con esquema extendido por medio de la interfaz web del iDRAC6" en la página 154.
4. Seleccione Objeto de dispositivo **iDRAC**.
5. Haga clic en **OK** (Aceptar).

Cómo crear un objeto de privilegio

NOTA: Se debe crear un objeto de privilegio en el mismo dominio que el objeto de asociación relacionado.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.
2. Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

   Se abre la ventana **Nuevo objeto**.
3. Introduzca un nombre para el nuevo objeto.
4. Seleccione **Objeto de privilegio**.
5. Haga clic en **OK** (Aceptar).
6. Haga clic con el botón derecho del mouse en el objeto de privilegio que creó y seleccione **Propiedades**.
7. Haga clic en la ficha **Privilegios de administración remota** y seleccione los privilegios que desee otorgar al usuario o grupo (ver Tabla 5-13).

Cómo crear un objeto de asociación

NOTA: El objeto de asociación del iDRAC6 se deriva de un grupo y su alcance está establecido en Local de dominio.

1. En la ventana **Raíz de consola** (MMC), haga clic con el botón derecho del mouse en un contenedor.

2 Seleccione **Nuevo→ Dell Remote Management Object Advanced**.

Esto abrirá la ventana **Nuevo objeto**.

3 Introduzca un nombre para el nuevo objeto.

4 Seleccione **Objeto de asociación**.

5 Seleccione el ámbito para el **objeto de asociación**.

6 Haga clic en **OK** (Aceptar).

7 Proporcione privilegios de acceso a los usuarios autentificados para acceder al objeto de asociación creado. Para hacer esto:

   a Vaya a **Herramientas administrativas→ Editar ADSI**. Aparecerá la ventana **Editar ADSI**.

   b En el panel derecho, navegue al objeto de asociación creado, haga clic con el botón derecho del mouse y seleccione **Propiedades**.

   c En la ficha **Seguridad**, haga clic en **Agregar**.

   d Escriba `Usuarios autentificados`, haga clic en **Comprobar nombres**, luego haga clic en **Aceptar**. Se agrega **Usuarios autentificados** a la lista de **Nombres de grupos y de usuarios**.

   e Haga clic en **OK** (Aceptar).

Cómo agregar objetos a un objeto de asociación

En la ventana **Propiedades de objeto de asociación**, puede asociar usuarios o grupos de usuarios, objetos de privilegio y dispositivos iDRAC6 o grupos de dispositivos iDRAC6.

Puede agregar grupos de usuarios y dispositivos de iDRAC6. El procedimiento para la creación de grupos relacionados con Dell y grupos ajenos a Dell es el mismo.

Cómo agregar usuarios o grupos de usuarios

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 Introducción el nombre del grupo de usuarios o del usuario y haga clic en **Aceptar**.

Cómo 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 cuando se autentifican en un dispositivo iDRAC6. Solo se puede agregar un objeto de privilegio a un objeto de asociación.

Cómo agregar dispositivos iDRAC6 o grupos de dispositivos iDRAC6

Para agregar dispositivos iDRAC6 o grupos de dispositivos iDRAC6:

1. Seleccione la ficha **Productos** y haga clic en **Agregar**.
2. Introduzca el nombre de los dispositivos iDRAC6 o de los grupos de dispositivos iDRAC6 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 un dispositivo iDRAC6 conectado a la red disponible para los usuarios o grupos de usuarios definidos. Puede agregar varios dispositivos iDRAC6 a un objeto de asociación.

Configuración de Active Directory de Microsoft con esquema extendido por medio de la interfaz web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC→ Red/Seguridad→** ficha **Servicio de directorio→ Microsoft Active Directory**.

   Aparece la pantalla de resumen de **Active Directory**.
4. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

   Aparece la pantalla **Paso 1 de 4 Active Directory**.
5. Para validar el certificado SSL de los servidores Active Directory, seleccione la casilla de verificación **Validación de certificados activada** en **Configuración de certificados**.

   Si no desea validar el certificado SSL de los servidores Active Directory, vaya al paso 7.

6 En **Cargar certificado de CA de Active Directory**, introduzca la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado y haga clic en **Cargar.**

NOTA: Debe escribir la ruta completa de acceso al archivo, que incluye la ruta completa de acceso y el nombre y la extensión completos del archivo.

La información para el certificado de CA de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.

7 Haga clic en **Next** (Siguiente).

Aparece la pantalla **Paso 2 de 4 de Configuración y administración de Active Directory**.

8 Seleccione la casilla de verificación **Active Directory activado**.

NOTA: En esta versión, la función de autenticación de dos factores (TFA) con tarjeta inteligente no puede utilizarse si Active Directory está configurado para el esquema extendido. La función de inicio de sesión único (SSO) se admite tanto para el esquema estándar como para el esquema extendido.

9 Haga clic en **Agregar** para introducir el **Nombre de dominio de usuario**. Introduzca el nombre del dominio en el campo de texto y luego haga clic en **Aceptar**. Tenga en cuenta que este paso es opcional. Si configura una lista de dominios de usuario, la lista estará disponible en la pantalla de inicio de sesión en la interfaz web. Puede elegir de la lista y luego sólo debe ingresar el nombre de usuario.

10 En el campo **Tiempo de espera,** ingrese la cantidad de segundos que desea que el iDRAC6 espere las respuestas de Active Directory.

11 Seleccione la opción **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory de una búsqueda en el DNS. Si ya están configuradas, las **Direcciones 1 a 3 del servidor del controlador de dominio** se ignoran. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. De lo contrario, seleccione la opción **Especificar un dominio** e introduzca el nombre del dominio para utilizar en la búsqueda en el DNS. iDRAC6 tratará de conectarse a cada una de las direcciones (las primeras 4 direcciones que encuentre la búsqueda de DNS), una a la vez, hasta establecer una conexión satisfactoriamente. Si se selecciona el **esquema extendido**, los controladores de dominio se encuentran donde están ubicados el objeto dispositivo iDRAC6 y los objetos de asociación.

Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.

NOTA: iDRAC6 no cuenta con protección contra fallas para los controladores de dominio especificados cuando falla la búsqueda en el DNS, pues de ser así ninguno de los servidores que ofrece la búsqueda en el DNS funciona.

12 Seleccione la opción **Especificar direcciones del controlador de dominio** para que el iDRAC6 pueda utilizar las direcciones especificadas del servidor del controlador de dominio de Active Directory. La búsqueda en el DNS no se realizó. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Al seleccionar la opción **Especificar direcciones del controlador de dominio**, es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. Si la opción **Esquema extendido** está seleccionada, las direcciones representan los controladores de dominio donde se encuentran el objeto dispositivo iDRAC6 y los objetos de asociación.

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 controlador de dominio si tiene activada la validación de certificado.

13 Haga clic en **Siguiente**.

Aparece la pantalla **Paso 3 de 4 de Configuración y administración de Active Directory**.

14 En **Selección de esquema**, seleccione la casilla de verificación **Selección de esquema extendido.**

15 Haga clic en **Siguiente**.

Aparece la pantalla **Paso 4 de 4 de Active Directory**.

16 En **Configuración del esquema extendido**, introduzca el **Nombre del iDRAC6** y el **Nombre de dominio del iDRAC6** para configurar el objeto de dispositivo iDRAC6 y su ubicación en Active Directory.

17 Haga clic en **Terminar** para guardar los cambios y luego en **Terminado**.

Aparece la página principal de resumen **Configuración y administración de Active Directory**. A continuación, pruebe los valores de Active Directory que ha configurado.

18 Desplácese hasta la parte inferior de la pantalla y haga clic en **Probar la configuración.**

Aparece la pantalla **Probar la configuración de Active Directory**.

19 Ingrese su nombre de usuario y contraseña del iDRAC6 y luego haga clic en **Iniciar prueba**.

Se mostrarán los resultados de la prueba y el registro de la prueba. Para obtener información adicional, ver "Prueba de las configuraciones realizadas" en la página 169.

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC6 para admitir el inicio de sesión en Active Directory. Vaya a la pantalla **Red** (haga clic en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Red**) para configurar el servidor(es) DNS manualmente o utilice DHCP para obtener el servidor(es) DNS.

Con este paso se completa la configuración de Active Directory con esquema extendido.

Configuración de Active Directory con esquema extendido por medio de RACADM

Use los siguientes comandos para configurar la función de Active Directory del iDRAC6 con esquema extendido por medio de la herramienta de interfaz de línea de comandos (CLI) de RACADM en lugar de la interfaz web.

1 Abra un símbolo del sistema y introduzca los siguientes comandos de RACADM:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config -g cfgActiveDirectory -o
cfgADRacName <nombre común del RAC>

racadm config -g cfgActiveDirectory -o
cfgADRacDomain <nombre completo del dominio
del RAC>

racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <nombre de dominio completo
o dirección IP del controlador de dominio>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <nombre de dominio completo
o dirección IP del controlador de dominio>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <nombre de dominio completo
o dirección IP del controlador de dominio>
```

NOTA: Debe configurar por lo menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. En el esquema extendido, se trata de las direcciones IP o el FQDN de los controladores de dominio donde se ubica el dispositivo iDRAC6. Los servidores del catálogo global no se utilizan en el modo de esquema extendido.

Si desea desactivar la validación del certificado durante el protocolo de enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

En este caso, no tiene que cargar un certificado de entidad emisora.

Si desea aplicar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

En este caso, deberá cargar un certificado de la entidad emisora con el siguiente comando de RACADM:

```
racadm sslcertupload -t 0x2 -f <certificado CA raíz
de ADS>
```

El siguiente comando de RACADM es opcional. Consulte "Importar el certificado SSL de firmware del iDRAC6" en la página 137 para obtener información adicional.

```
racadm sslcertdownload -t 0x1 -f <certificado raíz
SSL de RAC>
```

2 Si DHCP está activado en el iDRAC6 y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca el siguiente comando de RACADM:

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

3 Si DHCP está desactivado en el iDRAC6 o si desea introducir manualmente la dirección IP de DNS, introduzca los siguientes comandos de RACADM:

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<dirección IP del DNS primario>
```

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

4 Si desea configurar una lista de dominios de usuario para que solamente tenga que introducir el nombre de usuario cuando se inicia sesión en la interfaz web del iDRAC6, introduzca el siguiente comando:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName <nombre de dominio completo o
dirección IP del controlador de dominio> -i
<índice>
```

Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

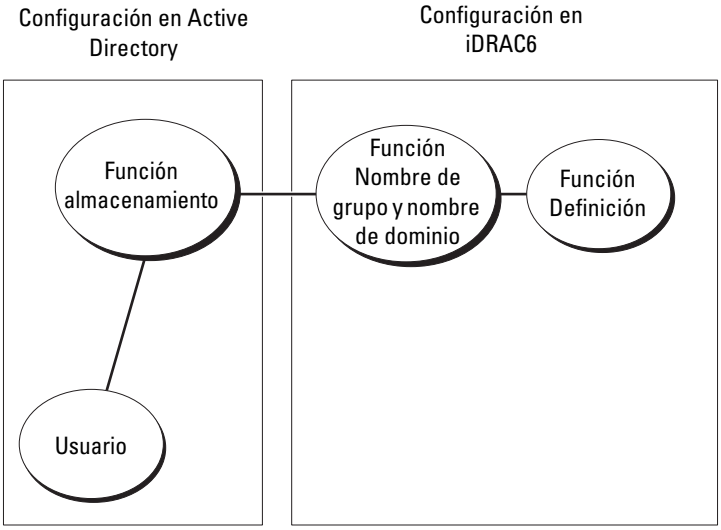
Ver "Uso del iDRAC6 con Microsoft Active Directory" en la página 133 para obtener información detallada sobre los dominios de usuario.

5 Presione **Intro** para completar la configuración de Active Directory con esquema extendido.

Generalidades del esquema estándar de Active Directory

Como se muestra en Ilustración 6-3, el uso del esquema estándar para la integración de Active Directory requiere configuración tanto en Active Directory como en iDRAC6.

Ilustración 6-3. Configuración del iDRAC6 con Active Directory de Microsoft y esquema estándar



En Active Directory se utiliza un objeto de grupo estándar como grupo de funciones. Un usuario con acceso al iDRAC6 será miembro del grupo de funciones. Para que este usuario tenga acceso a una tarjeta del iDRAC6 específica, es necesario configurar el nombre del grupo de funciones y el nombre de dominio en esa tarjeta del iDRAC6. A diferencia de la solución de esquema extendido, la función y el nivel de privilegios se definen en cada tarjeta del iDRAC6 y no en Active Directory. En cada iDRAC6, pueden configurarse y definirse hasta cinco grupos de funciones. La Tabla 6-9 muestra los privilegios predeterminados del grupo de funciones.

Tabla 6-9. Privilegios predeterminados del grupo de funciones

Grupos de funciones	Nivel predeterminado de privilegios	Permisos otorgados	Máscara de bits
Grupo de funciones 1	None	Iniciar sesión en el iDRAC, Configurar el iDRAC, Configurar usuarios, Borrar registros, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Probar alertas, Ejecutar comandos de diagnóstico	0x000001ff
Grupo de funciones 2	None	Iniciar sesión en el iDRAC, Configurar el iDRAC, Ejecutar comandos de control del servidor, Acceder a la consola virtual, Acceder a los medios virtuales, Alertas de prueba, Ejecutar comandos de diagnóstico	0x000000f9
Grupo de funciones 3	None	Inicio de sesión en iDRAC	0x00000001
Grupo de funciones 4	None	Sin permisos asignados	0x00000000
Grupo de funciones 5	None	Sin permisos asignados	0x00000000

NOTA: Los valores de la máscara de bits se utilizan únicamente cuando se establece el esquema estándar con RACADM.

Casos de dominio único y dominio múltiple

Si todos los usuarios y los grupos de funciones conectados, así como los grupos anidados, están en el mismo dominio, deben configurarse en el iDRAC6 sólo las direcciones de dominio de los controladores. En este caso de dominio único, se admiten todos los tipos de grupos.

Si todos los usuarios y los grupos de funciones conectados, o cualquiera de los grupos anidados, pertenecen a múltiples dominios, deben configurarse en el iDRAC6 las direcciones del servidor de catálogo global. En este caso de dominio múltiple, todos los grupos de función y grupos anidados, si los hubiera, deben ser del tipo Grupo universal.

Configuración de Active Directory con esquema estándar para acceder al iDRAC6

Debe realizar los pasos siguientes para configurar Active Directory antes de que los usuarios de Active Directory puedan acceder al iDRAC6:

1. En un servidor de Active Directory (controlador de dominio), abra el **complemento de usuarios y equipos de Active Directory**.
2. Cree un grupo o seleccione un grupo existente. Agregue el usuario de Active Directory como miembro del grupo de Active Directory para acceder al iDRAC6.
3. Configure el nombre del grupo y el nombre de dominio en el iDRAC6 utilizando la interfaz web o RACADM (ver "Configuración de Active Directory con esquema estándar mediante la interfaz web del iDRAC6" en la página 162 o "Configuración de Active Directory con esquema estándar vía RACADM" en la página 166).

Configuración de Active Directory con esquema estándar mediante la interfaz web del iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC→ Red/Seguridad→** ficha **Servicio de directorio→ Microsoft Active Directory**.

   Aparece la página de resumen de **Active Directory**.
4. Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

   Aparece la pantalla **Paso 1 de 4 Active Directory**.
5. En **Configuración de certificados**, seleccione **Validación de certificados activada**.
6. En **Cargar certificado de CA de Active Directory**, introduzca la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado y haga clic en **Cargar**.

   NOTA: Debe escribir la ruta completa de acceso al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

   La información para el certificado de CA de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.

7 Haga clic en **Siguiente**.

Aparece la pantalla **Paso 2 de 4 de Configuración y administración de Active Directory**.

8 Seleccione la casilla de verificación **Active Directory activado**.

9 Seleccione la opción **Inicio de sesión con tarjeta inteligente** para activar el inicio de sesión con tarjeta inteligente. Se le pedirá el inicio de sesión mediante tarjeta inteligente durante cualquier intento subsiguiente de inicio de sesión mediante la interfaz gráfica para usuario. Este campo es opcional.

10 Seleccione **Habilitar inicio de sesión único** si desea iniciar sesión en el iDRAC6 sin necesidad de introducir credenciales de autentificación de usuario de dominio, por ejemplo, nombre de usuario y contraseña.

11 Haga clic en **Agregar** para introducir el **Nombre de dominio de usuario**. Introduzca el nombre del dominio en el campo de texto y luego haga clic en **Aceptar**. Tenga en cuenta que este paso es opcional. Si configura una lista de dominios de usuario, la lista estará disponible en la pantalla de inicio de sesión en la interfaz web. Puede elegir de la lista y luego sólo debe ingresar el nombre de usuario.

12 En el campo **Tiempo de espera**, ingrese la cantidad de segundos que desea que el iDRAC6 espere las respuestas de Active Directory.

13 Seleccione la opción **Buscar controladores de dominio con DNS** para obtener los controladores de dominio de Active Directory de una búsqueda en el DNS. Si ya están configuradas, las **Direcciones 1 a 3 del servidor del controlador de dominio** se ignoran. Seleccione la opción **Dominio de usuario desde inicio de sesión** para realizar una búsqueda en el DNS con el nombre de dominio del usuario. De lo contrario, seleccione la opción **Especificar un dominio** e introduzca el nombre del dominio para utilizar en la búsqueda en el DNS. iDRAC6 tratará de conectarse a cada una de las direcciones (las primeras 4 direcciones que encuentre la búsqueda de DNS), una a la vez, hasta establecer una conexión satisfactoriamente. Si se selecciona el **esquema estándar**, los controladores de dominio se encuentran donde están ubicadas las cuentas de usuario y los grupos de funciones.

14 Seleccione la opción **Especificar direcciones del controlador de dominio** para que el iDRAC6 pueda utilizar las direcciones especificadas del servidor del controlador de dominio de Active Directory. La búsqueda en el DNS no se realizó. Especifique la dirección IP o el nombre de dominio completo (FQDN) de los controladores de dominio. Al seleccionar la opción **Especificar direcciones del controlador de dominio**, es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria.

Si la opción **esquema estándar** está seleccionada, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

NOTA: iDRAC6 no cuenta con protección contra fallas para los controladores de dominio especificados cuando falla la búsqueda en el DNS, pues de ser así ninguno de los servidores que ofrece la búsqueda en el DNS funciona.

15 Haga clic en **Siguiente**.

Aparece la pantalla **Paso 3 de 4 de Configuración y administración de Active Directory**.

16 En **Selección de esquema**, seleccione la casilla de verificación **Selección de esquema estándar**.

17 Haga clic en **Siguiente**.

Aparece la pantalla **Paso 4a de 4 de Active Directory**.

18 En **Configuración del esquema estándar**, seleccione la opción **Buscar servidores del catálogo global con DNS** e introduzca el nombre del dominio **raíz** para utilizar en una búsqueda en el DNS y obtener los servidores de catálogo global de Active Directory. Si ya están configuradas, las Direcciones 1 a 3 del servidor de Catálogo global se ignoran. iDRAC6 intenta conectarse a cada una de las direcciones (vuelve a las 4 primeras direcciones por la búsqueda en el DNS), una por una, hasta que logra una conexión satisfactoria El servidor de catálogo global sólo se requiere para el esquema estándar en caso de que las cuentas del usuario y los grupos de funciones tengan diferentes dominios.

NOTA: iDRAC6 no cuenta con protección contra fallas para los servidores de catálogo global especificados cuando falla la búsqueda en el DNS, pues de ser así ninguno de los servidores que ofrece la búsqueda en el DNS funciona.

19 Seleccione la opción **Especificar direcciones del servidor de catálogo global** e introduzca la dirección IP o el nombre de dominio completo (FQDN) de los servidores de catálogo global. La búsqueda en el DNS no se realizó. Es necesario configurar al menos una de las tres direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria.

NOTA: El servidor de catálogo global sólo es necesario para el esquema estándar cuando las cuentas de usuario y los grupos de funciones se encuentran en dominios diferentes. En el caso de este dominio múltiple, sólo se puede utilizar el grupo universal. Si utiliza la interfaz gráfica del usuario de web del iDRAC6 para configurar Active Directory, deberá introducir una dirección global aun si el usuario y el grupo pertenecen al mismo dominio.

20 Haga clic en un botón de **Grupo de función** para agregar un grupo de función.

Aparece la pantalla **Paso 4b de 4 Configurar grupo de funciones**.

21 Ingrese el **nombre del grupo**. El nombre del grupo identifica el grupo de funciones en Active Directory asociado con el iDRAC6.

22 Ingrese el **dominio del grupo**. El **Nombre de grupo** es el nombre del dominio raíz completamente expresado para el bosque.

23 En la sección **Privilegios del grupo de funciones**, defina los privilegios del grupo. Ver Tabla 5-13 para obtener información sobre los privilegios del grupo de funciones.

NOTA: Si modifica alguno de los permisos, el privilegio del grupo de funciones ya existente (Administrador, Usuario avanzado o Usuario invitado) cambiará al Grupo personalizado o al privilegio de grupo de funciones correspondiente según los permisos que se modifiquen.

24 Haga clic en **Aceptar** para guardar la configuración del grupo de funciones.

Aparece un diálogo de alerta que le indica que su configuración se ha modificado. Haga clic en **Aceptar** para volver a la pantalla **Paso 4a de 4, Configuración y administración de Active Directory**.

25 Para agregar un grupo de funciones adicional, repita los pasos paso 20 a paso 24.

26 Haga clic en **Terminar** y luego en **Terminado**.

Aparece la pantalla de resumen **Configuración y administración de Active Directory**. Pruebe los valores de Active Directory que ha configurado.

27 Desplácese hasta la parte inferior de la pantalla y haga clic en **Probar la configuración.**

Aparece la pantalla **Probar la configuración de Active Directory**.

28 Ingrese su nombre de usuario y contraseña del iDRAC6 y luego haga clic en **Iniciar prueba**.

Se mostrarán los resultados de la prueba y el registro de la prueba. Para obtener información adicional, ver "Prueba de las configuraciones realizadas" en la página 169.

NOTA: Debe tener un servidor DNS configurado correctamente en el iDRAC6 para admitir el inicio de sesión en Active Directory. Vaya a la pantalla **Red** (haga clic en **Sistema→ Configuración de iDRAC**, y luego en **Red/Seguridad→ ficha Red**) para configurar los servidores DNS de forma manual o utilizar DHCP para obtener los servidores DNS.

Ha completado la configuración de Active Directory con esquema estándar.

Configuración de Active Directory con esquema estándar vía RACADM

Use los siguientes comandos para configurar la función Active Directory del iDRAC6 con esquema estándar por medio de la interfaz de línea de comandos de RACADM en lugar de la interfaz web.

1 Abra un símbolo del sistema y introduzca los siguientes comandos de RACADM:

```
racadm config -g cfgActiveDirectory -o
cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgStandardSchema -i <índice> -o
cfgSSADRoleGroupName <nombre común del grupo de
funciones>

racadm config -g cfgStandardSchema -i <índice> -o
cfgSSADRoleGroupDomain <nombre de dominio
completo>

racadm config -g cfgStandardSchema -i <índice> -o
cfgSSADRoleGroupPrivilege <Bit Mask Value for
specific RoleGroup permissions>
```

NOTA: Para conocer los valores de máscara de bits para permisos de grupos de funciones específicos, ver Tabla 6-9.

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <nombre de dominio completo
o dirección IP del controlador de dominio>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <nombre de dominio completo
o dirección IP del controlador de dominio>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <nombre de dominio completo
o dirección IP del controlador de dominio>
```

NOTA: Ingrese el FQDN del controlador de dominio, *no* el FQDN del dominio. Por ejemplo, ingrese `nombredeservidor.dell.com` en vez de `dell.com`.

NOTA: Es necesario configurar al menos una de las 3 direcciones. iDRAC6 intenta conectarse a cada una de las direcciones configuradas, una por una, hasta lograr una conexión satisfactoria. En el esquema estándar, se trata de las direcciones de los controladores de dominio donde se ubican las cuentas de usuario y los grupos de funciones.

```
racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog1 <fully qualified domain name or IP
address of the domain controller>

racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog2 <fully qualified domain name or IP
address of the domain controller>

racadm config -g cfgActiveDirectory -o cfgGlobal
Catalog3 <fully qualified domain name or IP
address of the domain controller>
```

NOTA: Sólo es necesario el servidor de Catálogo global para el esquema estándar cuando las cuentas de usuario y los grupos de funciones se encuentran en dominios diferentes. En el caso de este dominio múltiple, sólo se puede utilizar 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 controlador de dominio si tiene activada la validación de certificado.

Si desea desactivar la validación del certificado durante el protocolo de enlace con SSL, ingrese el siguiente comando de RACADM:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

En este caso, no es necesario cargar ningún certificado de CA.

Si desea aplicar la validación del certificado durante el enlace con SSL, ingrese el siguiente comando de RACADM:

```
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 <certificado CA
raíz de ADS>
```

El siguiente comando de RACADM es opcional. Consulte "Importar el certificado SSL de firmware del iDRAC6" en la página 137 para obtener información adicional.

```
racadm sslcertdownload -t 0x1 -f <certificado raíz
SSL de RAC>
```

2 Si DHCP está activado en el iDRAC6 y desea utilizar el DNS proporcionado por el servidor DHCP, introduzca los siguientes comandos de RACADM:

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

3 Si el DHCP está desactivado en el iDRAC6 o si desea introducir manualmente la dirección IP de DNS, introduzca los siguientes comandos de RACADM:

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1
<dirección IP del DNS primario>
```

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

4 Si desea configurar una lista de dominios de usuario para que solamente tenga que introducir el nombre de usuario cuando se inicia sesión en la interfaz web, introduzca el siguiente comando:

```
racadm config -g cfgUserDomain -o
cfgUserDomainName <nombre de dominio completo o
dirección IP del controlador de dominio> -i
<índice>
```

Puede configurar hasta 40 dominios de usuario con números de índice entre 1 y 40.

Ver "Uso del iDRAC6 con Microsoft Active Directory" en la página 133 para obtener información acerca de dominios de usuario.

Prueba de las configuraciones realizadas

Si desea verificar si su configuración funciona o si desea diagnosticar el problema en caso de errores al iniciar sesión en Active Directory, puede realizar pruebas de la configuración en la interfaz web del iDRAC6.

Una vez definida la configuración en la interfaz web del iDRAC6, haga clic en **Probar la configuración** en la parte inferior de la pantalla. Deberá introducir un nombre de usuario de prueba (por ejemplo, **nombredeusuario@dominio.com**) y una contraseña para realizar la prueba. Según la configuración, completar todos los pasos de la prueba y mostrar los resultados de cada paso puede tardar un tiempo. Aparecerá un registro detallado de la prueba, en la parte inferior de la pantalla de resultados.

Si se produce un error en cualquiera de los pasos, examine la información que aparece en el registro de la prueba para identificar el error y su posible solución. Para obtener información sobre los errores más comunes, ver "Preguntas frecuentes" en la página 175.

Si desea efectuar cambios en la configuración, haga clic en la ficha **Active Directory** y modifique la configuración según las instrucciones detalladas.

Cómo utilizar el iDRAC6 con el servicio de directorios LDAP

iDRAC6 ofrece una solución genérica para admitir la autentificación basada en el protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP). Esta función no requiere una extensión del esquema en sus servicios de directorios.

Para que la implementación del LDAP en iDRAC6 sea genérica, se utilizan las características en común de distintos servicios de directorios para agrupar a los usuarios y asignar la relación usuario-grupo. La acción específica del servicio de directorio es el esquema. Por ejemplo, pueden tener distintos nombres de atributo para el grupo, el usuario y el vínculo entre el usuario y el grupo. Estas acciones se pueden configurar en iDRAC6.

Sintaxis de inicio de sesión (usuario de directorio y usuario local)

A diferencia de Active Directory, no se utilizan caracteres especiales ("@", "\", y "/") para diferenciar un usuario LDAP de un usuario local. El usuario que inicia sesión debe ingresar el nombre de usuario, excluyendo el nombre de dominio. iDRAC6 toma el nombre de usuario tal cual se indica y no lo desglosa en nombre de usuario y dominio del usuario.

Cuando se activa el LDAP genérico, iDRAC6 primero intenta conectar al usuario como usuario de directorio. Si esto falla, se activa la búsqueda de usuario local.

NOTA: No hay modificación de comportamiento en la sintaxis de inicio de sesión de Active Directory. Cuando se activa el LDAP genérico, la página de inicio de sesión de la interfaz gráfica del usuario muestra únicamente la opción **Este iDRAC** en el menú desplegable.

NOTA: En esta versión de lanzamiento, solamente se admiten los servicios de directorio basados en openLDAP, openDS, Novell eDir y Fedora. el nombre de usuario no permite los caracteres "<" y ">".

Configuración del servicio de directorio de LDAP genérico mediante la interfaz web de iDRAC6

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Haga clic en **Sistema**→ **Configuración de iDRAC**→ **Red/Seguridad** ficha→ **Servicio de directorio**→ **Servicio de directorio LDAP genérico**.
4. La página **Configuración y administración de LDAP genérico** muestra la configuración actual del LDAP genérico de iDRAC6. Desplácese hasta el final de la página **Configuración y administración de LDAP genérico** y haga clic en **Configurar LDAP genérico**.

   Aparece la página **Paso 1 de 3** de **Configuración y administración de LDAP genérico**. Use esta página para configurar el certificado digital que se utiliza durante el inicio de las conexiones de SSL al comunicarse con un servidor LDAP genérico. Estas comunicaciones usan el LDAP a través de SSL (LDAPS). Si activa la convalidación de certificados, cargue el certificado de la Autoridad de certificados (CA) que emitió el certificado utilizado por el servidor LDAP durante el inicio de las conexiones de SSL. El certificado de CA se usa para convalidar la autenticidad del certificado proporcionado por el servidor LDAP durante el inicio de SSL.

   NOTA: En esta versión, no se admite el enlace al LDAP basado en puertos distintos a SSL. Sólo se admite el LDAP a través de SSL.
5. En **Configuración de certificados**, seleccione **Activar validación de certificados** para activar la validación de certificados. Si esta opción está activada, iDRAC6 utiliza el certificado de CA para validar el certificado del servidor LDAP durante el enlace del nivel de conexión segura (SSL); si está desactivada, iDRAC6 omite el paso de validación de certificados del enlace de SSL. Es posible desactivar la validación de certificados durante las pruebas o si el administrador del sistema decide confiar en los controladores de dominio en el límite de seguridad sin validar sus certificados de SSL.

   PRECAUCIÓN: Asegúrese de que la opción CN = abrir LDAP FQDN esté configurada (por ejemplo: CN= openldap.lab) en el campo de asunto del certificado del servidor LDAP, durante la generación del certificado. El campo CN en el certificado del servidor debe estar configurado de tal forma que coincida con el campo de la dirección del servidor LDAP en iDRAC6 para que funcione la validación de certificados.

6 En **Cargar un certificado de CA de Active Directory**, escriba la ruta de acceso al archivo del certificado o examine el equipo para encontrarlo.

NOTA: Debe escribir la ruta de acceso absoluta al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

7 Haga clic en **Cargar**.

Se cargará el certificado de CA raíz que firma todos los certificados del servidor SSL de los controladores de dominio.

8 Haga clic en **Siguiente** para ir a la página **Paso 2 de 3 de Configuración y administración del LDAP genérico**. Use esta página para configurar la información de ubicación de los servidores de LDAP genérico y las cuentas de los usuarios.

NOTA: En esta versión, no se admite la función de autenticación de dos factores (TFA) con tarjeta inteligente ni la función de inicio de sesión único (SSO) para el servicio de directorio de LDAP genérico.

9 Seleccione la opción **Activar LDAP genérico**.

NOTA: En esta versión no se admite el grupo anidado. El firmware busca al miembro directo del grupo para que coincida con el DN del usuario. Además, sólo se admite un dominio único. No se admiten dominios cruzados.

10 Seleccione la opción **Usar nombre distinguido para buscar la pertenencia a grupos** para emplear el nombre distinguido (DN) como miembros del grupo. iDRAC6 compara el DN del usuario recuperado del directorio para compararlo con los miembros del grupo. Si esta opción no está seleccionada, el nombre de usuario proporcionado por el usuario se utiliza para compararlo con los miembros del grupo.

11 En el campo **Dirección del servidor LDAP**, introduzca el nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP. Para especificar múltiples servidores LDAP redundantes que sirven al mismo dominio, proporcione la lista de todos los servidores separados por comas. iDRAC6 intenta conectar a cada servidor, uno por uno, hasta que logra una conexión satisfactoria.

12 Introduzca el puerto usado por el LDAP a través de SSL en el campo **Puerto del servidor LDAP**. El valor predeterminado es 636.

13 En el campo **DN de enlace**, introduzca el DN de un usuario utilizado para enlazar al servidor durante la búsqueda del DN del usuario. Si no está especificado, se utiliza un enlace anónimo.

14 Introduzca la **Contraseña de enlace** para usarla junto con el **DN de enlace**. Esta opción es obligatoria si no se admite el enlace anónimo.

15 En el campo **DN de base para buscar**, introduzca el DN del subdirectorio donde deben iniciarse todas las búsquedas.

16 En el campo **Atributo de inicio de sesión del usuario**, introduzca el atributo del usuario a buscar. El valor predeterminado es UID. Se recomienda que este nombre sea único dentro del DN de base seleccionado, pues de lo contrario será necesario configurar un filtro de búsqueda para garantizar la singularidad del usuario. Si el DN del usuario no puede ser identificado en forma exclusiva por la combinación de búsqueda de atributo y filtro de búsqueda, el inicio de sesión falla.

17 En el campo **Atributo de pertenencia a grupo**, especifique qué atributo de LDAP debe utilizarse para verificar la pertenencia al grupo. Éste debe ser un atributo de la clase de grupos. Si no está especificado, iDRAC6 usa los atributos de *miembro* y *miembro único*.

18 En el campo **Filtro de búsqueda**, introduzca un filtro de búsqueda de LDAP válido. Use el filtro si el atributo del usuario no logra identificar de forma exclusiva al usuario dentro del DN de base seleccionado. Si no está especificado, el valor predeterminado es *objectClass*=*, que busca todos los objetos en el árbol. Este filtro de búsqueda adicional configurado por el usuario se aplica únicamente para la búsqueda de DN del usuario y no para la búsqueda de pertenencia de grupo.

19 Haga clic en **Siguiente** para ir a la página **Paso 3a de 3** de **Configuración y administración del LDAP genérico**. Use esta página para configurar los grupos de privilegios utilizados para autorizar a los usuarios. Al activar el LDAP genérico, se utilizan grupos de funciones para especificar la política de autorización para los usuarios de iDRAC6.

20 En **Grupos de funciones**, haga clic en un **Grupo de funciones**.

Aparece la página **Paso 3b de 3 de Configuración y administración de LDAP genérico**. Use esta página para configurar cada grupo de funciones empleado para controlar la política de autorizaciones de los usuarios.

21 Introduzca el **Nombre distintivo (DN) del grupo** que identifica al grupo de funciones en el servicio de directorio de LDAP genérico que está vinculado con el iDRAC6.

22 En la sección **Privilegios del grupo de funciones**, especifique los privilegios asociados con el grupo seleccionando la opción **Nivel de privilegio del grupo de funciones**. Por ejemplo, si selecciona **Administrador**, se seleccionan todos los privilegios para dicho nivel de permiso.

23 Haga clic en **Aplicar** para guardar la configuración del grupo de funciones.

El Web Server de iDRAC6 automáticamente lo llevará de regreso a la página **Paso 3a de 3 de Configuración y administración de LDAP genérico** donde aparece la configuración de su grupo de funciones.

24 Configure grupos de funciones adiciones de ser necesario.

25 Haga clic en **Terminar** para volver a la página de resumen de **Configuración y administración de LDAP**.

26 Haga clic en **Comprobar configuración** para verificar la configuración del LDAP genérico.

27 Escriba el nombre de usuario y la contraseña de un usuario del directorio seleccionado para comprobar la configuración del LDAP. El formato depende del *Atributo de inicio de sesión del usuario* que se utilice, y el nombre de usuario introducido debe coincidir con el valor del atributo seleccionado.

NOTA: Al comprobar la configuración de LDAP con la opción **Activar validación de certificados** marcada, iDRAC6 requiere la identificación del servidor LDAP a través del nombre de dominio completo (FQDN) y no una dirección IP. Si el servidor LDAP es identificado por una dirección IP, la validación de certificados falla, ya que el iDRAC6 no logra comunicarse con el servidor LDAP.

Aparecen los resultados de la prueba y el registro de la misma. Ha completado la configuración del **servicio de directorio del LDAP genérico**.

Preguntas frecuentes

Problemas de inicio de sesión en Active Directory

Iniciar sesión en el iDRAC6 a través del inicio de sesión único de Active Directory lleva aproximadamente 4 minutos.

Si bien el inicio de sesión único normal de Active Directory generalmente demora menos de 10 segundos, puede demorar unos 4 minutos para iniciar sesión en el iDRAC6 a través del inicio de sesión único de Active Directory si especificó el **servidor DNS preferido** y el **servidor DNS alternativo** en la página **Red** del iDRAC6, y el servidor DNS preferido falló. Hay tiempos de espera de DNS cuando un servidor DNS no funciona. El iDRAC6 posibilita el inicio de sesión a través del servidor DNS alternativo.

Configuré Active Directory para un dominio presente en Active Directory de Windows Server 2008 y definí estas configuraciones. Un dominio secundario o subdominio se encuentra presente para el dominio, el usuario y el grupo están presentes en el mismo dominio secundario, y el usuario es miembro de ese grupo. Ahora bien, si intento iniciar sesión en el iDRAC6 mediante el usuario presente en el dominio secundario, el inicio de sesión único de Active Directory falla.

Esto puede deberse a que el tipo de grupo es incorrecto. Existen dos tipos de grupos en el servidor de Active Directory:

- **Seguridad**: los grupos de seguridad permiten administrar el acceso de usuarios y equipos a los recursos compartidos y filtrar la configuración de la política de grupo.
- **Distribución**: los grupos de distribución tienen la finalidad de utilizarse sólo como listas de distribución por correo electrónico.

Procure siempre que el tipo de grupo sea **Seguridad**. No es posible utilizar grupos de distribución para asignar permisos para ningún objeto ni utilizarlos para filtrar la configuración de política de grupo.

No puedo iniciar sesión en Active Directory, ¿qué debo hacer?

iDRAC6 proporciona una herramienta de diagnóstico en la interfaz web.

1. Inicie sesión como usuario local con privilegios de administrador en la interfaz web.

2 En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC→ Red/Seguridad→** ficha **Servicio de directorio→ Microsoft Active Directory**.

Aparece la pantalla de resumen de **Active Directory**.

3 Desplácese hasta la parte inferior de la pantalla y haga clic en **Probar la configuración.**

Aparece la pantalla **Probar la configuración de Active Directory**.

4 Ingrese un nombre de usuario de prueba y su contraseña, luego haga clic en **Iniciar prueba**.

iDRAC6 ejecuta la prueba paso a paso y muestra el resultado de cada paso. iDRAC6 también registra el resultado detallado de la prueba para ayudarlo a resolver problemas.

Si persisten los problemas, configure los valores de Active Directory, cambie la configuración de usuario y vuelva a ejecutar la prueba hasta que el usuario de prueba apruebe el paso de autorización.

Activé la validación de certificados pero no puedo iniciar sesión en Active Directory. Ejecuté los diagnósticos de la interfaz gráfica de usuario y los resultados de la prueba muestran el siguiente mensaje de error. ¿Cuál puede ser el problema y cómo lo soluciono?

```
ERROR: No se puede establecer conexión con el
servidor LDAP, error:14090086:SSL
rutinas:SSL3_GET_SERVER_CERTIFICATE:error en la
validación de certificados: verifique que se haya
cargado en el iDRAC el certificado correcto de la
autoridad de certificados (CA). Verifique también
si la fecha del iDRAC se encuentra dentro
del periodo válido de los certificados y
si la dirección del controlador de dominio
configurada en el iDRAC concuerda con el sujeto
del certificado del servidor de Active Directory.
```

Si la validación de certificados está activada, el iDRAC6 utiliza el certificado de la CA cargado para verificar el certificado del servidor de directorio cuando el iDRAC6 establece la conexión SSL con el servidor de directorio. Los motivos más frecuentes de error en la validación de certificados son:

- La fecha del iDRAC6 no se encuentra dentro del período válido del certificado del servidor o del certificado de CA. Verifique la hora del iDRAC6 y el período válido del certificado.
- Las direcciones del controlador de dominio configuradas en el iDRAC6 no concuerdan con el sujeto o con el nombre alternativo del sujeto del certificado del servidor de directorio.
  - Si está utilizando una dirección IP, ver "Estoy utilizando una dirección IP para una dirección de controlador de dominio y no puedo validar el certificado. ¿Cuál es el problema?" en la página 178.
  - Si utiliza un FQDN, asegúrese de estar utilizando el FQDN del controlador de dominio y no el dominio. Por ejemplo, use `nombredeservidor.ejemplo.com` y *no* `ejemplo.com`.

¿Qué debo verificar si no puedo iniciar sesión en el iDRAC6 con Active Directory?

Primero, diagnostique el problema con la función Probar la configuración. Para obtener instrucciones, ver "No puedo iniciar sesión en Active Directory, ¿qué debo hacer?" en la página 175.

Luego, solucione el problema detallado en el resultado de la prueba. Para obtener información adicional, ver "Prueba de las configuraciones realizadas" en la página 169.

Los problemas más frecuentes se explican en esta sección. Sin embargo, en general, debe verificar lo siguiente:

1. Asegúrese de utilizar el nombre del dominio de usuario correcto durante un inicio de sesión y no el nombre NetBIOS.
2. Si tiene una cuenta de usuario del iDRAC6 local, inicie sesión en el iDRAC6 con las credenciales locales.
   a. Asegúrese de que la casilla de verificación **Active Directory activado** esté seleccionada en la página **Paso 2 de 4 Configuración y administración de Active Directory**.

b Si activó la validación de certificados, asegúrese de haber cargado el certificado raíz de CA correcto de Active Directory en el iDRAC6. El certificado aparece en el área **Certificado de CA de Active Directory** actual. Asegúrese de que la hora del iDRAC6 se encuentre dentro del período de vigencia del certificado de CA.

c Si está utilizando el esquema extendido, asegúrese de que **Nombre del iDRAC6** y **Nombre de dominio del iDRAC6** coincidan con la configuración del entorno de Active Directory.

Si está utilizando el esquema estándar, asegúrese de que **Nombre de grupo** y **Dominio del grupo** coincidan con la configuración de Active Directory.

d Vaya a la pantalla **Red**. Seleccione **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Red**.
Compruebe que la configuración del DNS sea correcta.

e Verifique los certificados de controlador de dominio SSL para asegurarse de que la hora del iDRAC6 esté dentro del plazo de vigencia del certificado.

Validación del certificado de Active Directory

Estoy utilizando una dirección IP para una dirección de controlador de dominio y no puedo validar el certificado. ¿Cuál es el problema?

Verifique el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio. Generalmente, Active Directory utiliza el nombre del host, no la dirección IP, del controlador de dominio en el campo Sujeto o Nombre alternativo de sujeto del certificado de controlador de dominio.

Puede solucionar el problema por medio de estas acciones:

- Configure el nombre del host (FQDN) del controlador de dominio como las *direcciones del controlador de dominio* en el iDRAC6 para que coincidan con el Sujeto o el Nombre alternativo de sujeto del certificado del servidor.
- Vuelva a emitir el certificado del servidor de forma tal que use una dirección IP en el campo Sujeto o Nombre alternativo de sujeto que concuerde con la dirección IP configurada en el iDRAC6.
- Desactive la validación de certificados si prefiere confiar en este controlador de dominio sin validación de certificados durante el protocolo de enlace SSL.

¿Por qué el iDRAC6 activa la validación de certificados de manera predeterminada?

El iDRAC6 aplica fuertes medidas de seguridad para asegurar la identidad del controlador de dominio al que se conecta el iDRAC6. Sin la validación de certificados, un pirata informático podría falsificar un controlador de dominio y controlar la conexión SSL. Si decide confiar en todos los controladores de dominio de su límite de seguridad sin validación de certificado, puede desactivarla por medio de la interfaz gráfica del usuario o la interfaz de línea de comandos.

Esquema extendido y esquema estándar

Estoy utilizando un esquema extendido en un entorno de dominio múltiple. ¿Cómo configuro las direcciones de controlador de dominio?

Use el nombre del host (FQDN) o la dirección IP de los controladores de dominio donde reside el objeto iDRAC6.

¿Necesito configurar una dirección de Catálogo global?

Si está utilizando un esquema extendido, no puede configurar direcciones de catálogo global, ya que no se utilizan con éste.

Si está utilizando un esquema estándar, y los usuarios y grupos de funciones pertenecen a dominios distintos, debe configurar las direcciones de catálogo global. En este caso, sólo puede utilizar el grupo universal.

Si está utilizando un esquema estándar, y todos los usuarios y grupos de funciones se encuentran en el mismo dominio, no es necesario configurar direcciones de catálogo global.

¿Cómo funciona la consulta del esquema estándar?

iDRAC6 se conecta primero a las direcciones de controlador de dominio configuradas. Si tanto el usuario como el grupo de funciones residen en ese dominio, los privilegios se guardan.

Si se configuran direcciones de controlador global, iDRAC6 continúa consultando el catálogo global. Si se recuperan privilegios adicionales del catálogo global, estos privilegios se acumulan.

Varios

¿El iDRAC6 siempre usa LDAP a través de SSL?

Sí. Todo el transporte se realiza mediante el puerto seguro 636 ó 3269.

Durante la *prueba de la configuración*, el iDRAC6 efectúa una CONEXIÓN A LDAP sólo para ayudar a aislar el problema pero no se vincula a LDAP con una conexión insegura.

¿Admite el iDRAC6 el nombre NetBIOS?

No en esta versión.

7

Configuración de iDRAC6 para el inicio de sesión único y mediante tarjeta inteligente

Esta sección brinda información para configurar iDRAC6 para iniciar sesión mediante tarjeta inteligente para usuarios locales y usuarios de Active Directory, y para el inicio de sesión único (SSO) para usuarios de Active Directory.

iDRAC6 admite la autentificación de Active Directory con Kerberos para permitir el inicio de sesión único (SSO) y con tarjeta inteligente en Active Directory.

Acerca de la autentificación basada en Kerberos

Kerberos es un protocolo de autentificación de red que permite que los sistemas se comuniquen de forma segura a través de una red sin protección. Para ello, los sistemas deben demostrar su autenticidad. Para mantener los más altos estándares de cumplimiento de autentificación, el iDRAC6 ahora admite la autentificación de Active Directory con Kerberos para permitir el inicio de sesión único (SSO) y con tarjeta inteligente en Active Directory.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista y Windows Server 2008 usan Kerberos como su método de autentificación predeterminado.

El iDRAC6 utiliza Kerberos para admitir dos tipos de mecanismos de autentificación: El inicio de sesión único y mediante tarjeta inteligente en Active Directory. Para el inicio de sesión único, el iDRAC6 emplea las credenciales de usuario almacenadas en caché en el sistema operativo al iniciar sesión mediante una cuenta válida de Active Directory.

Para el inicio de sesión con tarjeta inteligente de Active Directory, el iDRAC6 utiliza la autentificación de dos factores (TFA) con tarjeta inteligente a modo de credenciales para permitir el inicio de sesión en Active Directory.

La autentificación de Kerberos en el iDRAC6 fallará si la hora del iDRAC6 difiere de la hora del controlador de dominio. Se permite una diferencia máxima de 5 minutos. Para permitir una autentificación correcta, sincronice la hora del servidor con la hora del controlador de dominio y después **restablezca** el iDRAC6.

También puede utilizar el siguiente comando de diferencia de zona horaria de RACADM para sincronizar la hora:

```
racadm config -g cfgRacTuning -o
cfgRacTuneTimeZoneOffset <offset value>
```

Prerrequisitos para el inicio de sesión único y la autentificación mediante tarjeta inteligente de Active Directory

Los prerrequisitos tanto para el inicio de sesión único como para la autentificación mediante tarjeta inteligente de Active Directory son:

- Configure el iDRAC6 para el inicio de sesión de Active Directory. Para obtener más información, consulte "Uso del servicio de directorio de iDRAC6" en la página 133.
- Registre el iDRAC6 como equipo en el dominio raíz de Active Directory.
  - **a** Haga clic en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ subficha Red**.
  - **b** Indique una dirección IP de **servidor DNS alternativo/preferido** que sea válida. Este valor señala la dirección IP del servidor DNS que forma parte del dominio raíz, que autentifica las cuentas de Active Directory de los usuarios.
  - **c** Seleccione **Registrar el iDRAC6 en el DNS**.
  - **d** Indique un **nombre de dominio DNS** válido.
  - **e** Verifique que la configuración de DNS de la red coincida con la información de DNS de Active Directory.

    Consulte la ayuda en línea del iDRAC6 para obtener más información.

- Para permitir el uso de los dos nuevos mecanismos de autentificación, el iDRAC6 admite la configuración para activarse como si fuera un servicio de Kerberos en una red Kerberos de Windows. La configuración de Kerberos en el iDRAC6 requiere los mismos pasos que la configuración de un servicio Kerberos externo a Windows Server como principal función de seguridad en Windows Server Active Directory.

  La herramienta **ktpass** de Microsoft (proporcionada por Microsoft como parte del CD/DVD de instalación del servidor) se utiliza para crear el enlace del nombre principal de servicio (SPN) a una cuenta de usuario y exportar la información de confianza a un archivo *keytab* de Kerberos de tipo MIT, lo que permite establecer una relación de confianza entre un usuario o sistema externo y el centro de distribución de claves (KDC). El archivo keytab contiene una clave criptográfica que se usa para cifrar la información entre el servidor y el KDC. La herramienta ktpass permite el uso de servicios basados en UNIX que admiten la autentificación Kerberos para ejecutar las funciones de interoperabilidad proporcionadas por un servicio Kerberos KDC de Windows Server.

  El archivo keytab que se obtiene de la utilidad ktpass está disponible para el iDRAC6 como archivo para cargar y está activado para actuar como un servicio kerberizado en la red.

  Como el iDRAC6 es un dispositivo con sistema operativo distinto a Windows, ejecute la utilidad **ktpass** (que es parte de Microsoft Windows) en el controlador de dominio (servidor Active Directory) donde desea asignar el iDRAC6 a una cuenta de usuario de Active Directory.

  Por ejemplo, utilice el comando **ktpass** siguiente para crear el archivo keytab de Kerberos:

  ```
  C:\> ktpass.exe -princ HTTP/
  idracname.domainname.com@DOMAINNAME.COM -mapuser
  DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5
  -ptype KRB5_NT_PRINCIPAL -pass <password> +DesOnly
  -out c:\krbkeytab
  ```

  NOTA: Si tiene algún problema con el usuario de iDRAC6 para quien se crea el archivo keytab, cree un nuevo usuario y un nuevo archivo keytab. Si se ejecuta nuevamente el mismo archivo keytab que se creó inicialmente, no se configurará correctamente.

Después de que el comando anterior se ejecute correctamente, ejecute el siguiente comando:

```
C:\>setspn -a HTTP/idracname.domainname.com
username
```

El tipo de cifrado admitido por el iDRAC6 para la autentificación con Kerberos es DES-CBC-MD5. El tipo principal es KRB5_NT_PRINCIPAL. Las propiedades de la cuenta del usuario a la que está asignado el nombre principal de servicio deben tener activada la propiedad Utilizar los tipos de cifrado DES para esta cuenta.

NOTA: Debe crear una cuenta de usuario de Active Directory para usar con la opción -mapuser del comando **ktpass**. Además, debe tener el mismo nombre que el nombre del iDRAC6 en el DNS para el que cargará el archivo keytab generado.

NOTA: Se recomienda usar la utilidad **ktpass** más reciente para crear el archivo keytab. Además, al generar el archivo keytab, use letras *minúsculas* para el **nombre_de_idrac** y el **nombre principal de servicio**.

Este procedimiento generará un archivo keytab que deberá cargar en el iDRAC6.

NOTA: Este archivo contiene una clave de cifrado y debe guardarse de manera segura.

Para obtener más información acerca de la utilidad **ktpass**, visite el sitio web de Microsoft: **http://technet.microsoft.com/en-us/library/cc779157(WS.10).aspx**

- La hora del iDRAC6 debe sincronizarse con el controlador de dominio de Active Directory.

Configuración del explorador para activar el inicio de sesión único de Active Directory

Para configurar los valores del explorador para Internet Explorer:

1. Abra el explorador web de Internet Explorer.
2. Seleccione **Herramientas→ Opciones de Internet→ Seguridad→ Intranet local**.
3. Haga clic en **Sitios**.

4 Seleccione las siguientes opciones solamente:
   - Incluya todos los sitios locales (intranet) no enumerados en otras zonas.
   - Incluya todos los sitios que omiten el servidor proxy.
5 Haga clic en **Advanced** (Opciones avanzadas).
6 Agregue todos los nombres de dominio relativos que se usarán en instancias del iDRAC y que forman parte de la configuración del SSO (por ejemplo: mihost.ejemplo.com.)
7 Haga clic en **Cerrar** y luego en **Aceptar**.
8 Haga clic en **OK** (Aceptar).

Para configurar los valores del explorador para Firefox:

1 Abra el explorador de web Firefox.
2 En la barra de dirección, introduzca `about:config`.
3 En **Filtro**, introduzca `network.negotiate`.
4 Agregue el nombre de iDRAC a network.negotiate-auth.trusted-uris (usando lista de valores separados por coma).
5 Agregue el nombre de iDRAC a network.negotiate-auth.trusted-uris (usando lista de valores separados por coma).

Uso de SSO de Active Directory

Puede configurar el iDRAC6 para utilizar el protocolo de autentificación de red Kerberos a fin de activar el inicio de sesión único. Para obtener más información acerca de cómo configurar el iDRAC6 para usar esta función, ver "Prerrequisitos para el inicio de sesión único y la autentificación mediante tarjeta inteligente de Active Directory" en la página 182.

Configuración del iDRAC6 para utilizar el inicio de sesión único

1 Asegúrese de que tiene lo siguiente:
   a Creado el objeto de dispositivo, el objeto de privilegio y el objeto de asociación en el servidor Active Directory.
   b Establecer los privilegios de acceso para el objeto de privilegio creado. Se recomienda no proporcionar privilegios de administrador ya que así se podrían omitir ciertos controles de seguridad.

c Asocie el objeto de dispositivo y el objeto de privilegio con el objeto de asociación.

d Agregue el usuario de SSO (usuario con acceso) anterior al objeto de dispositivo.

e Proporcione privilegio de acceso a *Usuarios autentificados* para acceder al objeto de asociación creado.

Para obtener más información acerca de cómo realizar estos pasos, ver "Cómo agregar usuarios y privilegios del iDRAC6 a Active Directory" en la página 151.

2 Abra una ventana de un explorador web compatible.

3 Inicie sesión en la interfaz web del iDRAC6.

4 En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC→ Red/Seguridad→** ficha **Red**. Seleccione la página **Red** y verifique si el **Nombre del iDRAC6 en el DNS** es correcto y coincide con el nombre usado para nombres de dominio completos del iDRAC6.

5 En el árbol del sistema, seleccione **Sistema→ Configuración de iDRAC→ Red/Seguridad→** ficha **Servicio de directorio → Microsoft Active Directory**.

Aparece la pantalla de resumen de **Active Directory**.

6 Desplácese hasta la parte inferior de la pantalla y haga clic en **Configurar Active Directory**.

Aparece la pantalla **Configuración y administración de Active Directory Paso 1 de 4**.

7 Para validar el certificado SSL de los servidores Active Directory, seleccione la casilla **Activar validación de certificados** en **Configuración de certificados**.

Si no desea validar el certificado SSL de los servidores Active Directory, no realice ninguna acción; proceda al paso 9.

8 En **Cargar certificado de CA de Active Directory**, introduzca la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado y haga clic en **Cargar.**

NOTA: Debe escribir la ruta completa de acceso al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo.

La información para el certificado de CA de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.

9 Haga clic en **Next** (Siguiente).

Aparece la pantalla **Configuración y administración de Active Directory Paso 2 de 4**.

10 Seleccione la casilla de marcación **Activar Active Directory**.

11 Seleccione **Activar inicio de sesión único** si desea iniciar sesión en el iDRAC6 directamente después de conectar la estación de trabajo sin necesidad de introducir credenciales de autentificación de usuario de dominio, por ejemplo, nombre de usuario y contraseña.

Para iniciar sesión en el iDRAC6 por medio de esta función, es necesario haber iniciado sesión en el sistema por medio de una cuenta de usuario de Active Directory válida. Además, también se requiere haber configurado la cuenta de usuario para iniciar sesión en el iDRAC6 por medio de las credenciales de Active Directory. El iDRAC6 utiliza las credenciales de Active Directory guardadas en la caché para permitir el inicio de sesión.

Para activar la función de SSO por medio de CLI, ejecute el siguiente comando RACADM:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

12 Agregue el **nombre de dominio del usuario** e introduzca la dirección IP de la dirección de servidor del controlador de dominio. Seleccione la opción **Buscar controladores de dominio con DNS** o la opción **Especificar direcciones del controlador de dominio**. Seleccione **Next** (Siguiente). Aparece la pantalla **Configuración y administración de Active Directory Paso 3 de 4**.

13 Seleccione la opción **Esquema estándar** o **Esquema ampliado** y haga clic en **Siguiente**.

Si seleccionó **Esquema estándar**, vaya al paso 13. Si seleccionó **Esquema ampliado**, vaya al paso 14.

14 Para esquema estándar:

a En la pantalla **Paso 4a de 4 de Active Directory**, escriba la dirección IP del **Servidor de catálogo global** o seleccione la opción **Buscar servidores de catálogo global con DNS** y escriba el **Nombre del dominio raíz** para realizar una búsqueda en el DNS y obtener los servidores de catálogo global activos.

b Haga clic en cualquiera de los grupos de funciones y agregue la información del grupo de funciones de la que el usuario válido de Active Directory es miembro. Aparece la pantalla **Active Directory Paso 4b de 4**.

c Escriba el nombre del grupo de funciones, el nivel de privilegios del grupo de funciones y los privilegios necesarios y haga clic en **Terminar**. Aparece el mensaje "La configuración se definió correctamente." Haga clic en **OK** (Aceptar). La pantalla **Paso 4a de 4** muestra el nombre del grupo de funciones creado, el dominio del grupo y el nivel de privilegios del grupo.

d Haga clic en **Terminar**. Aparece el mensaje de ejecución satisfactoria.

15 Para esquema ampliado, en la pantalla **Active Directory Paso 4 de 4**, escriba el **Nombre del iDRAC6** y el **Nombre del dominio del iDRAC6** y haga clic en **Terminar**. Aparece el mensaje de ejecución satisfactoria.

Inicio de sesión en iDRAC6 mediante inicio de sesión único

1 Inicie sesión en la estación de administración mediante su cuenta de red de Active Directory válida.

2 Inicie sesión en la página web del iDRAC6 mediante el nombre de dominio completo del iDRAC6:

http://nombre_del_idrac.dominio.com.

El iDRAC6 iniciará su sesión por medio de las credenciales que quedaron almacenadas en caché en el sistema operativo cuando inició sesión con una cuenta de red válida de Active Directory.

Configuración de la autentificación de tarjeta inteligente

El iDRAC6 admite la función de autentificación por medio de dos factores (TFA) al activar el **inicio de sesión mediante tarjeta inteligente**.

Los esquemas tradicionales de autentificación utilizan nombres de usuario y contraseñas para autentificar a los usuarios. Esto proporciona una seguridad mínima.

En cambio, la función TFA proporciona mayor seguridad porque los usuarios deben proporcionar dos factores de autentificación, el que poseen y el que conocen. El factor que se posee es la tarjeta inteligente, un dispositivo físico, y el factor que se conoce es un código secreto, como una contraseña o PIN.

La autentificación de dos factores requiere que los usuarios verifiquen su identidad cuando proporcionan *ambos* factores.

Configuración del Inicio de sesión mediante tarjeta inteligente en el iDRAC6

Para activar la función de inicio de sesión mediante tarjeta inteligente del iDRAC6 desde la interfaz web:

1. Abra una ventana de un explorador web compatible.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Aparece la pantalla **Paso 1 de 4 de Configuración y administración de Active Directory**.
4. Para validar el certificado SSL de los servidores Active Directory, seleccione la casilla **Validación de certificados activada** en **Configuración de certificados**. Si no desea validar el certificado SSL de los servidores Active Directory, vaya directamente a paso 6.
5. En **Cargar certificado de CA de Active Directory**, introduzca la ruta de acceso al archivo del certificado o examine el equipo para encontrar el archivo del certificado y haga clic en **Cargar.** Debe escribir la ruta completa de acceso al archivo, que incluye la ruta de acceso completa y el nombre y la extensión completos del archivo. La información para el certificado de CA de Active Directory que cargó aparece en la sección **Certificado actual de CA de Active Directory**.

6. Haga clic en Siguiente. Aparece la pantalla **Paso 2 de 4 de Configuración y administración de Active Directory**.
7. Seleccione la casilla de verificación **Active Directory activado**.
8. Seleccione **Activar inicio de sesión mediante tarjeta inteligente** para activar el inicio de sesión mediante tarjeta inteligente. Se le pedirá el inicio de sesión mediante tarjeta inteligente durante cualquier intento subsiguiente de inicio de sesión mediante la interfaz gráfica de usuario.
9. Agregue el **nombre de dominio del usuario** e introduzca la dirección IP de la dirección de servidor del controlador de dominio. Seleccione **Next** (Siguiente).
10. Seleccione **Configuración del esquema estándar** en la página **Paso 3 de 4 Configuración y administración de Active Directory**. Seleccione **Next** (Siguiente).
11. En la página **Paso 4a de 4 Active Directory**, introduzca la dirección IP del **Servidor de catálogo global**. Agregue la información de grupo de funciones del cual es miembro su usuario válido de Active Directory seleccionando uno de los grupos de funciones (página **Paso 4B de 4 Configurar grupo de funciones**). Introduzca el **nombre del grupo**, el **dominio del grupo** y los **privilegios del grupo de funciones**. Seleccione **Aceptar** y luego **Terminar**. Después de seleccionar **Listo**, desplácese hasta la parte inferior de la página **Active Directory** y seleccione **Carga del archivo keytab de Kerberos**.
12. Cargue un archivo keytab de Kerberos que sea válido. Asegúrese de que las horas del servidor de Active Directory y del iDRAC6 estén sincronizadas. Antes de cargar el archivo keytab, verifique que la hora y la zona horaria sean las correctas. Para obtener más información acerca de cómo crear un archivo keytab, ver "Configuración de iDRAC6 para el inicio de sesión único y mediante tarjeta inteligente" en la página 181.

Deseleccione la opción **Activar inicio de sesión mediante tarjeta inteligente** para desactivar la función de inicio de sesión mediante tarjeta inteligente con TFA. La próxima vez que inicie sesión en la interfaz gráfica de usuario del iDRAC6, se le pedirá un nombre de usuario y una contraseña local o de Microsoft Active Directory, lo cual sucede como petición de inicio de sesión predeterminada de la interfaz web.

Inicio de sesión en el iDRAC6 mediante la autentificación con tarjeta inteligente de Active Directory

NOTA: De acuerdo con la configuración del explorador, el sistema puede solicitarle que descargue e instale el complemento ActiveX para lector de tarjeta inteligente cuando utiliza esta función por primera vez.

1. Inicie sesión en el iDRAC6 usando https.

   `https://<dirección IP>`

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

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

   donde *`dirección IP`* es la dirección IP del iDRAC6 y *`número de puerto`* corresponde al número de puerto HTTPS.

   La página de inicio de sesión del iDRAC6 aparecerá y le solicitará que inserte la tarjeta inteligente.

2. Inserte la tarjeta inteligente.
3. Introduzca el PIN y haga clic en **Iniciar sesión**.

   De esta forma habrá iniciado sesión en el iDRAC6 con sus credenciales de la forma en que están definidas en Active Directory.

   NOTA: Para mantener la sesión activa, no es necesario que la tarjeta inteligente permanezca en el lector.

Preguntas frecuentes acerca del inicio de sesión único

El inicio de sesión en Windows 7 y Windows Server 2008 R2 falla.

Debe activar los tipos de cifrado DES_CBC_CRC y DES_CBC_MD5 para Windows 7 y Windows Server 2008 R2. Para activar los tipos de cifrado:

1. Inicie sesión como administrador o como usuario con privilegios administrativos.
2. Vaya a **Inicio** y ejecute **gpedit**. Aparece la ventana **Editor de política de grupo local**.

3 Vaya a **Configuración del equipo local→ Configuración de Windows→ Configuración de seguridad→ Políticas locales→ Opciones de seguridad**.

4 Haga clic con el botón derecho del mouse en **Seguridad de la red: Configuración de los tipos de cifrado permitidos para Kerberos** y seleccione **Propiedades**.

5 Active todas las opciones y haga clic en **Aceptar**.

Solución de problemas de inicio de sesión mediante tarjeta inteligente en el iDRAC6

Utilice los siguientes consejos y sugerencias como ayuda para depurar una tarjeta inteligente que no permite el acceso:

Toma casi 4 minutos iniciar sesión en el iDRAC6 a través del inicio de sesión mediante tarjeta inteligente de Active Directory.

El inicio de sesión normal mediante tarjeta inteligente de Active Directory demora menos de 10 segundos, pero puede tardar casi 4 minutos para iniciar sesión en el iDRAC6 mediante tarjeta inteligente de Active Directory si especificó el **servidor DNS preferido** y el **servidor DNS alternativo** en la página **Red** del iDRAC6, pero falló el servidor DNS preferido. Hay tiempos de espera de DNS cuando un servidor DNS no funciona. El iDRAC6 posibilita el inicio de sesión a través del servidor DNS alternativo.

El complemento ActiveX no puede detectar el lector de tarjetas inteligentes

Verifique que la tarjeta inteligente sea compatible con el sistema operativo Microsoft Windows. Windows admite una cantidad limitada de proveedores de servicios de cifrado (CSP) de tarjetas inteligente.

Sugerencia: Como verificación general para determinar si los CSP de tarjetas inteligentes están presentes en un cliente particular, inserte la tarjeta inteligente en el lector en la pantalla de inicio de sesión (Ctrl-Alt-Supr) de Windows y revise si Windows detecta esa tarjeta y muestra el cuadro de diálogo para introducir el PIN.

PIN incorrecto de la tarjeta inteligente

Revise si la tarjeta inteligente se bloqueó debido a que se hicieron demasiados intentos con PIN incorrectos. En tales casos, el emisor de la tarjeta inteligente en la organización podrá ayudarle a obtener una nueva tarjeta inteligente.

No se puede iniciar sesión en el iDRAC6 como usuario de Active Directory

- Si no puede iniciar sesión en el iDRAC6 como usuario de Active Directory, trate de hacerlo sin activar el inicio de sesión mediante tarjeta inteligente. Puede desactivar el inicio de sesión mediante tarjeta inteligente a través de RACADM por medio del siguiente comando:

  ```
  racadm config -g cfgSmartCard -o
  cfgSmartCardLogonEnable 0
  ```

- Para plataformas Windows de 64 bits, el complemento de autentificación del iDRAC6 no se instalará correctamente si se encuentra instalada una versión de 64 bits del paquete redistribuible de Microsoft Visual C++ 2005. Debe instalar la versión de 32 bits del paquete redistribuible de Microsoft Visual C++ 2005 para que el complemento se instale y se ejecute correctamente.
- Si recibe el siguiente mensaje de error "`No es posible cargar el complemento de tarjeta inteligente. Verifique la configuración de IE o podría tener privilegios insuficientes para usar el complemento de tarjeta inteligente`", luego instale el paquete redistribuible Microsoft Visual C++ 2005. Este archivo está disponible en el sitio web de Microsoft en **microsoft.com**. Se han probado dos versiones distribuidas del paquete redistribuible de C++, las cuales permiten que se cargue el complemento de tarjeta inteligente de Dell:

Tabla 7-1. Versiones distribuidas del paquete redistribuible de C++

Nombre de archivo del paquete redistribuible	Version (Versión)	Fecha de publicación	Tamaño	Descripción
vcredist_x86.exe	6.0.2900.2180	21 de marzo de 2006	2.56 MB	MS Redistributable 2005
vcredist_x86.exe	9.0.21022.8	7 de noviembre de 2007	1.73 MB	Redistribuible 2008 de Microsoft

- Asegúrese de que la hora del iDRAC6 y la del controlador de dominio en el servidor del controlador de dominio no presenten más de 5 minutos de diferencia para que funcione la autentificación con Kerberos. Consulte la **hora del iDRAC6** en la página **Sistema→ Configuración de iDRAC→ Propiedades→ Información de acceso remoto** y la hora del controlador de dominio haciendo clic con el botón derecho del mouse en la hora en el extremo inferior derecho de la pantalla. La diferencia de zona horaria se muestra en el cuadro emergente. Para la hora estándar central (CST) de los EE.UU., la diferencia es –6. Use el siguiente comando RACADM de diferencia de zona horaria para sincronizar la hora del iDRAC6 (a través de RACADM remoto o Telnet/SSH): `racadm config -g cfgRacTuning –o cfgRacTuneTimeZoneOffset <offset value in minutes>.` Por ejemplo, si la hora del sistema es GMT -6 (CST de los EE. UU.) y la hora es 2 p.m., establezca la hora del iDRAC6 en la hora GMT 18:00, lo cual requeriría que introduzca "360" en el comando anterior para especificar la diferencia. También puede usar `cfgRacTuneDaylightoffset` para activar la variación de horario de verano. Esto evita tener que cambiar la hora dos veces al año cuando se realizan los ajustes de horario de verano, o simplemente calcúlelo en la diferencia anterior usando "300" en el ejemplo que antecede.

8

Visualización de la configuración y la condición del servidor administrado

System Summary (Resumen del sistema)

La página **Resumen del sistema** le permite visualizar la condición del sistema y otra información básica del iDRAC6 y le proporciona vínculos de acceso a las páginas de condición e información del sistema. Además, desde esta página puede iniciar rápidamente tareas comunes y ver los sucesos recientes registrados en Registro de sucesos del sistema (SEL).

Para acceder a la página **Resumen del sistema**, haga clic en **Sistema**→ ficha **Propiedades**→ **Resumen del sistema**. Consulte la *Ayuda en línea del iDRAC6* para obtener información detallada acerca de cada sección de la página **Resumen del sistema**.

Detalles del sistema

La página **Resumen del sistema** muestra información sobre los siguientes componentes del sistema:

- Gabinete del sistema principal
- Integrated Dell Remote Access Controller 6: Enterprise

Gabinete del sistema principal

Información del sistema

Esta sección de la interfaz web del iDRAC6 proporciona la siguiente información básica acerca de el servidor administrado:

- Descripción: el número de modelo o el nombre del servidor administrado.
- Versión BIOS: el número de versión del BIOS del servidor administrado.
- Etiqueta de servicio: el número de etiqueta de servicio del servidor.
- Código de servicio rápido: el número de código de servicio del sistema. Es la representación numérica decimal de la Etiqueta de servicio.

- Nombre del host: el nombre del host DNS asociado con el servidor administrado.
- Nombre del sistema operativo: el nombre del sistema operativo instalado en el servidor administrado.

  NOTA: El campo **Nombre del sistema operativo** se completa sólo si Dell OpenManage Server Administrator está instalado en el sistema administrado. Representan una excepción los nombres de sistemas operativos VMware, que se muestran aun si Server Administrator no está instalado en el sistema administrado. En ciertos sistemas operativos, la operación de actualización del nombre del sistema operativo en iDRAC puede tardar varios minutos después del inicio del servidor.
- Revisión del sistema: el número de revisión del chasis.
- Firmware de Lifecycle Controller: la versión del firmware de Lifecycle Controller.

Tarjeta mezzanine de E/S

Esta sección de la interfaz web del iDRAC6 proporciona la siguiente información acerca de las tarjetas mezzanine de E/S instaladas en el servidor administrado:

- Ubicación: enumera las tarjetas mezzanine de E/S instaladas en el servidor administrado. La lista también muestra las tarjetas mezzanine de E/S para plataformas que admiten tarjetas de expansión.
- Estado de presencia: indica si se encuentra o no la tarjeta mezzanine, o si es una extensión de la ranura para tarjeta mezzanine de otra red Fabric.
- Tipo de tarjeta: el tipo físico de tarjeta/conexión mezzanine instalada.
- Nombre del modelo: el número, tipo o descripción del modelo de las tarjetas mezzanine instaladas.

Tarjeta de almacenamiento integrada

Esta sección de la interfaz web del iDRAC6 proporciona información acerca de la tarjeta integrada de controlador de almacenamiento que se encuentra instalada en el servidor administrado:

- Tipo de tarjeta: muestra el nombre de modelo de la tarjeta de almacenamiento instalada, por ejemplo, SAS6/iR

Tarjeta de red integrada

Esta sección de la interfaz web del iDRAC6 proporciona información acerca de la tarjeta de red integrada que se encuentra instalada en el servidor administrado: Se muestra solo para determinadas plataformas.

- Tipo de tarjeta: muestra el tipo de tarjeta de la tarjeta de red integrada instalada en la placa, por ejemplo, Gigabit Ethernet.
- Nombre de modelo: muestra el nombre de modelo de la tarjeta de red integrada.

Para obtener más información acerca de la tarjeta de red integrada, consulte el *Manual del propietario de hardware* disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Recuperación automática

Esta sección de la interfaz web del iDRAC6 detalla el modo de operación actual de la función de recuperación automática del servidor administrado según la configuración de Open Manage Server Administrator:

- Acción de recuperación: acción a realizar cuando se detecta una falla o *bloqueo* en el sistema. Las acciones disponibles son Sin **acción**, **Restablecimiento forzado**, **Apagar** o **Ciclo de encendido**.
- Cuenta regresiva inicial: la cantidad de tiempo (en segundos) después de la detección de un bloqueo de sistema en que el iDRAC6 realiza una acción de recuperación.
- Cuenta regresiva actual: el valor actual (en segundos) del temporizador.

Integrated Dell Remote Access Controller 6: Enterprise

Información del iDRAC6

Esta sección de la interfaz web del iDRAC6 suministra la siguiente información acerca del iDRAC6:

- Fecha/hora: muestra la fecha y hora actuales (del momento de la última actualización de la página) del iDRAC6.
- Versión del firmware: muestra la versión actual del firmware del iDRAC6 instalada en el sistema administrado.
- Versión de CPLD: muestra la versión del dispositivo lógico programable complejo (CPLD) de la placa base.

- Versión de CPLD ampliada: muestra la versión del CPLD de la placa ampliada.
- Actualización del firmware: muestra la fecha y hora de la última actualización satisfactoria del firmware del iDRAC6.
- Dirección MAC: muestra la dirección MAC asociada con el controlador de interfaz de red de LOM (LAN de la placa base) del iDRAC6.

Configuración de IPv4

- Activado: muestra si está activada o desactivada la compatibilidad con el protocolo IPv4.

  NOTA: La opción del protocolo IPv4 está activada de manera predeterminada.
- DHCP activado: activado si el iDRAC6 está configurado para tomar su dirección IP e información asociada de un servidor DHCP.
- Dirección IP: muestra la dirección IP asociada con el iDRAC6 (no el servidor administrado).
- Máscara de subred: muestra la máscara de subred TCP/IP configurada para el iDRAC6.
- Puerta de enlace: muestra la dirección IP de la puerta de enlace de red configurada para el iDRAC6.
- Usar DHCP para obtener direcciones de servidor DNS: muestra si se utiliza el DHCP para obtener direcciones del servidor DNS.
- Servidor DNS preferido: muestra el servidor DNS primario actualmente activo.
- Servidor DNS alternativo: muestra la dirección del servidor DNS alternativo.

Configuración de IPv6

- Activado: muestra si está activada o desactivada la compatibilidad con el protocolo IPv6.
- Configuración automática activada: muestra si la configuración automática está activada o desactivada.
- Dirección de vínculo local: muestra la dirección IPv6 para el NIC del iDRAC6.

- Dirección de IPv6 1-16: muestra hasta 16 direcciones IPv6 (Dirección IPv6 1a dirección IPv6 16) para el NIC del iDRAC6.
- Puerta de enlace: muestra la dirección IP de la puerta de enlace de red configurada para el iDRAC6.
- Usar DHCPv6 para obtener direcciones del servidor DNS: muestra si se utiliza el DHCP para obtener direcciones del servidor DNS.
- Servidor DNS preferido: muestra el servidor DNS primario actualmente activo.
- Servidor DNS alternativo: muestra la dirección del servidor DNS alternativo.

NOTA: Esta información también se encuentra disponible en **Sistema→ iConfiguración de iDRAC→ Propiedades→ Información de acceso remoto.**

Direcciones MAC del NIC incorporado

- NIC 1: muestra las direcciones de control de acceso al medio (MAC) del controlador de interfaz de red (NIC) incorporado 1.

  Las direcciones MAC identifican de forma particular cada nodo de una red en la capa de control de acceso al medio.

  El NIC de la interfaz estándar de equipos pequeños de Internet (iSCSI) es un controlador de interfaces de red con la pila de iSCSI ejecutándose en el equipo host.

  Los NIC de Ethernet admiten el estándar de Ethernet cableado y enchufado en el bus del sistema del servidor.
- NIC 2: muestra las direcciones MAC del NIC 2 incorporado que lo identifica de forma particular en la red.
- NIC 3: muestra las direcciones MAC del NIC 3 incorporado que lo identifica de forma particular en la red. Es probable que las direcciones MAC del NIC 3 incorporado no aparezcan en todos los sistemas.
- NIC 4: muestra las direcciones MAC del NIC 4 incorporado que lo identifica de forma particular en la red. Es probable que las direcciones MAC del NIC 4 incorporado no aparezcan en todos los sistemas.

Las direcciones MAC del NIC incorporado devueltas por el comando `getSysInfo` de racadm y las direcciones MAC que se muestran bajo **Sistema→ Propiedades→ Detalles del sistema** son las direcciones MAC asignadas por el servidor. Si las direcciones MAC se administran remotamente o han sido asignadas por el chasis, las direcciones MAC activas se muestran bajo **Sistema→ Propiedades→ WWN/MAC**.

WWN/MAC

Haga clic en **Sistema→** ficha **Propiedades→ WWN/MAC** para ver la configuración actual de las tarjetas mezzanine de E/S instaladas y sus redes Fabric relacionadas. También puede ver las direcciones MAC asignadas remotamente. Si la función FlexAddress está activada en el CMC, las direcciones MAC persistentes asignadas globalmente (asignadas por el chasis) reemplazarán a los valores de cableado de cada LOM.

Condición del servidor

Haga clic en **Sistema→ ficha Propiedades→ Resumen del sistema**. En la sección **Estado del servidor**, puede hacer clic en los enlaces para ver información importante sobre el estado del iDRAC6 y los componentes supervisados por el iDRAC6. La columna de **Estado** muestra el estado de cada componente. Para obtener una lista de símbolos de estado y su significado, ver Tabla 19-3. Haga clic en el nombre del componente en la columna **Componente** para obtener información más detallada acerca de éste.

NOTA: La información del componente también puede obtenerse con un clic sobre su nombre en el panel izquierdo de la ventana. Los componentes permanecen visibles en el panel izquierdo independientemente de la ficha/pantalla seleccionada.

Las siguientes secciones explican detalladamente los enlaces del componente disponibles en la sección **Estado del servidor**.

iDRAC6

La pantalla **Información de acceso remoto** enumera una serie de detalles importantes acerca del iDRAC6, como el nombre, la revisión del firmware, la actualización del firmware, la hora del iDRAC6, la versión de IPMI, la versión de CPLD, el tipo de servidor y los parámetros de la red. Se puede acceder a los detalles adicionales haciendo clic sobre la ficha correspondiente ubicada en la parte superior de la pantalla.

La **hora del iDRAC** muestra la hora del BIOS o la hora de CMC. Cuando el sistema se reinicia, el BIOS envía la hora al iDRAC. Si el sistema host se enciende cuando se inicia el iDRAC, éste obtiene la hora del BIOS. Si el sistema host no se enciende cuando se inicia el iDRAC, éste obtendrá la hora del CMC. Es decir, el BIOS es la fuente preferida, lo cual significa que para obtener la hora del BIOS, el servidor host tiene que estar encendido.

La marca de tiempo del firmware siempre coincide con la última marca de tiempo del iDRAC obtenida anterior a la actualización de firmware, la cual puede ser la hora del BIOS si el sistema ha sido iniciado o reiniciado antes de la actualización del firmware o la hora de CMC.

CMC

La pantalla **CMC** muestra el estado de condición, la revisión del firmware y las direcciones IP de Chassis Management Controller. También puede iniciar la interfaz web del CMC con un clic sobre el botón **Iniciar interfaz web del CMC**. Consulte la *Guía del usuario de firmware de Chassis Management Controller* para obtener más información.

NOTA: Al iniciar la interfaz gráfica del usuario de web del CMC desde el iDRAC6, la búsqueda tendrá el mismo formato de dirección IP. Por ejemplo, si abre la interfaz gráfica del usuario de web del iDRAC6 con formato de dirección IPv6, la página web del CMC también abrirá una dirección IPv6 válida.

Baterías

La pantalla **Baterías** muestra el estado de la batería de tipo botón de la placa de sistema que mantiene el reloj en tiempo real (RTC) y el almacenamiento de los datos de configuración del CMOS del sistema administrado.

Temperatures

La pantalla **Temperaturas** muestra el estado y las lecturas de la sonda de temperatura ambiente integrada. Se muestran los umbrales de temperatura mínima y máxima para estados de *advertencia* y *falla*, junto con la condición actual de la sonda.

NOTA: Según el modelo del servidor, es posible que no se muestren los umbrales de temperatura para los estados de *advertencia* y *falla* y/o la condición de la sonda.

Voltajes

La pantalla **Sondas de voltaje** muestra el estado y las lecturas de estas sondas e informa acerca del estado del riel de voltaje incorporado y los sensores de núcleo de la CPU.

Supervisión de alimentación

La pantalla **Supervisión de alimentación** permite ver la siguiente información de supervisión y estadísticas de alimentación:

- Supervisión de alimentación: muestra la cantidad de energía (valor promedio en un minuto, medido en vatios de corriente alterna) que está utilizando el servidor de acuerdo con lo informado por el monitor actual de la placa de sistema.
- Amperaje: muestra el consumo actual (corriente alterna en amperios) en la unidad de suministro de energía activa.
- Estadísticas de seguimiento de alimentación: informa la cantidad de energía utilizada por el sistema desde el último restablecimiento de la lectura.
- Estadísticas pico: informa la cantidad pico de energía utilizada por el sistema desde el último restablecimiento de la lectura.
- Consumo de alimentación: muestra el consumo de energía mínimo, promedio y máximo, así como las fechas y horas de alimentación máximas y mínimas en el sistema para el minuto, la hora, el día y la semana últimos.
- Mostrar gráfica: muestra una representación gráfica del consumo de alimentación para 1 hora, 24 horas, 3 días y 1 semana.

NOTA: La alimentación y el amperaje se miden en corriente alterna.

CPU

La pantalla **CPU** informa la condición de cada CPU en el servidor administrado. Este estado de condición es un resumen de pruebas individuales térmicas, funcionales y de alimentación.

POST

La pantalla **Código de la Post** muestra el último código de la POST del sistema (en hexadecimales) antes del inicio del sistema operativo del servidor administrado.

Condiciones diversas

La pantalla **Condiciones diversas** proporciona acceso a los siguientes registros del sistema:

- Registro de sucesos del sistema: muestra los sucesos críticos de sistema que se producen en el sistema administrado.
- Código de la Post: muestra el último código de la post del sistema (en hexadecimales) antes del inicio del sistema operativo del servidor administrado.
- Pantalla de último bloqueo: muestra la pantalla y la hora de bloqueo más recientes.
- Captura de inicio: proporciona una reproducción de las últimas tres pantallas de inicio.

NOTA: Esta información también está disponible en **Sistema**→ ficha **Registros**→ **Registro de sucesos del sistema**.

Inventario del sistema

La página **Inventario del sistema** muestra los componentes del hardware y el firmware instalados en el sistema administrado.

Para acceder a la página Inventario del sistema, haga clic en **Sistema**→ **Propiedades**→ **Inventario del sistema**.

La sección **Inventario de hardware** muestra la información de los componentes que incluyen el iDRAC, la controladora RAID instalada, todas las CPU instaladas, todos los DIMM instalados, todos los HDD instalados, los NIC host (integrados e incorporados), la tarjeta de vídeo instalada y la tarjeta SD si está instalada.

La sección **Inventario de firmware** muestra la versión de firmware para los componentes de firmware e incluye el BIOS, la versión de Lifecycle Controller (USC) y el firmware del iDRAC.

Cada campo puede mostrar solamente un máximo de 48 caracteres. Si es mayor a 48, se truncará la cadena.

Para obtener más información, consulte la *Ayuda en línea de iDRAC6*.

Para asegurarse de que la función de Inventario de sistemas está funcionando, haga lo siguiente:

1. El sistema debe estar configurado para recopilar el inventario del sistema. Para ello, sírvase de la utilidad ROM de la Opción de iDRAC durante el inicio del sistema (Ctrl-E). En el menú **Servicios del sistema**, active la opción **Recopilar inventario del sistema al reiniciar (CSIOR)**.
2. Despues de haber activado CSIOR, el sistema host se reinicia y da comienzo, en la pantalla de salida, llegando al final del inicio del BIOS, se muestra el mensaje "Recopilando inventario del sistema" tras varios minutos.
3. Después del reinicio del host y la recopilación del inventario del sistema, reinicie iDRAC solamente.
4. Se puede acceder al inventario del hardware una vez que el iDRAC se haya iniciado.

   Después del reinicio del iDRAC, los componentes internos necesarios para atender las peticiones que proporcionan el inventario del hardware no se encontrarán listos de manera inmediata. Por lo tanto, espere 5 minutos tras el reinicio, y, a continuación, conecte al iDRAC para presentar el inventario del hardware. Esta operación puede tardar varios minutos después del primer restablecimiento del iDRAC. De manera alternativa, utilice WSMAN para comprobar la disponibilidad de los Servicios remotos en el iDRAC y poder determinar el momento en el que estará listo el inventario del hardware. Para su invocación, utilice el método GetRSStatus de la clase DCIM_LCService. Para obtener más detalles, consulte el MOF de servicio LC DCIM de Dell disponible en **delltechcenter.com**. El Servicio remoto debe estar disponible antes de que el inventario del hardware se encuentre listo, situación que estará directamente asociada a si el iDRAC ha sido reiniciado (paso 3) o no.

Solución de problemas

La página de Inventario de hardware muestra que la información de dicho inventario no se encuentra disponible.

Asegúrese de que se hayan seguido los pasos para la correcta activación del inventario de hardware. Esto incluye el tiempo de espera mínimo en el iDRAC antes de intentar mostrar la página tras un reinicio del iDRAC. Cualquier reinicio del iDRAC (incluida la actualización de firmware) requerirá este tiempo de espera mínimo. Ejecute la comprobación WSMAN sobre la disponibilidad de los Servicios remotos para comprobar el momento en el que se encontrará listo el inventario de hardware.

Al inventario de hardware le faltan algunos valores de atributo de hardware.

Es posible que algunos valores no hayan sido correctamente rellenados en el componente de hardware, por lo que se quedarán en blanco los campos de los elementos subyacentes que reúnen la información. Esto se verá reflejado en la GUI. La GUI del iDRAC mostrará la información que obtiene correctamente. Si faltan datos, los mismos faltaran en el inventario de hardware de USC. Si el componente de hardware admite el reacoplamiento, intente reacoplarlo para ver si se soluciona el problema. Si el componente de hardware admite el intercambio, cámbielo y el problema se habrá solucionado. Después de haber cambiado o reacoplado un componente, asegúrese de ejecutar CSIOR y utilice la comprobación WSMAN sobre la disponibilidad de Servicios remotos antes de intentar ver el inventario actualizado.

La mayoría del inventario de hardware contiene información en blanco y carece de muchos componentes admitidos.

Normalmente este problema se produce por la falta de activación de la función CSIOR o por la pérdida de datos provenientes de una recopilación anterior. Para reunir la información completa del inventario, deje que el sistema se inicie y asegúrese de que la función CSIOR esté activada en el sistema de configuración Ctrl-E de los Servicios remotos. Durante el inicio del sistema asegúrese de que la pantalla muestra el mensaje “Recopilando inventario del sistema” antes de que el host se inicie.

Falta información de inventario del firmware o la versión LC de la página Resumen del sistema y Detalles del sistema aparece como No se encuentra.

En este caso una opción sería el reinicio del iDRAC. También es posible que sea necesario actualizar el firmware del iDRAC incluso si la actualización es para el firmware recientemente instalado.

9

Configuración y uso de la comunicación en serie en la LAN

La comunicación en serie en la LAN (SOL) es una función de IPMI que permite que los datos de consola basados en texto de un servidor administrado, en lugar de enviarse al puerto de E/S serie como se haría en forma tradicional, se envíen a través de la red de administración Ethernet fuera de banda dedicada del iDRAC6. La consola fuera de banda de SOL permite que los administradores de sistemas administren de manera remota la consola de texto del servidor Blade desde cualquier lugar con acceso a la red. Los beneficios de SOL son los siguientes:

- Acceder de manera remota a los sistemas operativos sin tiempo de espera.
- Realizar diagnósticos de sistemas host en servicios de administración de emergencia (EMS) o en la consola administrativa especial (SAC) para Windows o un shell de Linux.
- Ver el progreso de un servidor Blade durante la autoprueba de encendido (POST) y reconfigurar el programa de configuración del BIOS (mientras se dirige a un puerto serie).

Activación de la comunicación en serie en la LAN del BIOS

Para configurar un servidor para la comunicación en serie en la LAN, es necesario llevar a cabo los pasos de configuración que se describen detalladamente a continuación.

1. Configurar la comunicación en serie en la LAN en el BIOS (opción desactivada de manera predeterminada)
2. Configurar el iDRAC6 para la comunicación en serie en la LAN
3. Seleccionar un método para inicializar la comunicación en serie en la LAN (SSH, Telnet, proxy SOL o herramienta IPMI)
4. Configurar el sistema operativo para SOL

De manera predeterminada, la comunicación serie está **desactivada** en el BIOS. Para redirigir los datos de la consola de texto del host a la comunicación en serie sobre LAN, debe activar la consola virtual a través de COM1.

Para cambiar la configuración del BIOS:

1. Inicie el servidor administrado.
2. Presione <F2> para acceder a la utilidad de configuración del BIOS durante la autoprueba de encendido.
3. Desplácese hacia abajo hasta llegar a Comunicación serie y presione <Intro>.

   En la ventana emergente, la lista de comunicación serie aparece con las siguientes opciones:

   - Apagado
   - Encendido sin consola virtual
   - Encendido con consola virtual

   Utilice las teclas de flecha para recorrer las opciones.
4. Asegúrese de que la opción **Encendido con consola virtual** esté activada. Asegúrese de que la opción **Dirección del puerto serie** sea COM1.
5. Verifique que el valor de **Velocidad en baudios a prueba de fallas** sea idéntico al valor de la velocidad en baudios de SOL configurada en el iDRAC6. El valor predeterminado de la velocidad en baudios a prueba de fallas y la velocidad en baudios de SOL configurada en el iDRAC6 es 115,2 kbps.
6. Asegúrese de que la opción **Redirección después de inicio** esté activada. Esta opción activa la redirección de SOL del BIOS en los reinicios subsecuentes. El BIOS cuenta con los valores VT100/VT220 y ANSI para **Tipo de terminal remota**.
7. Guarde los cambios y salga.

   El servidor administrado se reinicia.

Configuración de la comunicación en serie en la LAN en la interfaz gráfica del usuario de web del iDRAC6

1. Abra la pantalla **Configuración de la comunicación en serie en la LAN** seleccionando **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Comunicación en serie en la LAN**.
2. Verifique que la opción **Activar comunicación en serie en la LAN** esté seleccionada (activada). De manera predeterminada, la opción se encuentra activada.
3. Desde el menú desplegable **Velocidad en baudios**, seleccione la velocidad en baudios de SOL de la herramienta IPMI (velocidad de los datos). Las opciones son 9600 bps, 19,2 kbps, 57,6 kbps y 115,2 kbps. El valor predeterminado es 115,2.
4. Desde el menú desplegable **Límite de nivel de privilegio del canal**, seleccione un límite de nivel de privilegio para SOL.

NOTA: Asegúrese de que la velocidad en baudios de SOL sea idéntica al valor de la opción Velocidad en baudios a prueba de fallas definida en el BIOS.

5. Haga clic en **Aplicar** para guardar los valores.
6. Haga clic en **Advanced Settings** (Configuración avanzada). Aparecerá la pantalla **Configuración avanzada de la comunicación en serie en la LAN**, la cual le permitirá ajustar el rendimiento de SOL. Vea la Tabla 9-1.

Tabla 9-1. Valores de la pantalla de configuración avanzada de la comunicación en serie en la LAN

Valor	Descripción
Intervalo de acumulación de caracteres	Es la cantidad típica de tiempo que el iDRAC6 espera antes de enviar un paquete de datos parcial de SOL. Este parámetro se expresa en milisegundos. Se recomienda utilizar 10 milisegundos para obtener un rendimiento óptimo.

Tabla 9-1. Valores de la pantalla de configuración avanzada de la comunicación en serie en la LAN *(continuación)*

Valor	Descripción
Umbral de envío de caracteres	Indica la cantidad de caracteres por paquete de datos de SOL. Cuando la cantidad de caracteres aceptados por el iDRAC6 es igual o superior al valor de umbral de envío de caracteres, el iDRAC6 comienza a transmitir de inmediato paquetes de datos de SOL que contienen una cantidad de caracteres igual o inferior a dicho valor. Si un paquete contiene menos caracteres que lo expresado por este valor, se define como un paquete de datos de SOL parcial. Se recomienda utilizar 255 caracteres para obtener un rendimiento óptimo.

NOTA: Si cambia estos valores por otros menores, la función de consola virtual de SOL puede reducir su rendimiento. Aun más, la sesión de SOL deberá aguardar para recibir una confirmación por cada paquete antes de enviar el siguiente. En consecuencia, el rendimiento disminuirá.

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

8 Configure SSH y Telnet para SOL en **Sistema→ Configuración de iDRAC→ Red/Seguridad→** ficha **Servicios**.

NOTA: Cada servidor Blade admite sólo una sesión SOL activa.

NOTA: El protocolo SSH está activado de manera predeterminada. El protocolo Telnet está desactivado de manera predeterminada.

9 Haga clic en **Servicios** para abrir la pantalla **Servicios**.

NOTA: Los programas SSH y Telnet proporcionan acceso a través de un sistema remoto.

10 Haga clic en **Activado** en **SSH** o **Telnet** según sea necesario.

11 Haga clic en **Aplicar**.

NOTA: SSH es el método recomendado debido a sus mejores mecanismos de cifrado y seguridad.

NOTA: La duración de la sesión de SSH/Telnet puede ser infinita si el valor de tiempo de espera se establece en 0. El valor predeterminado es 1800 segundos.

12 Active la interfaz fuera de banda del iDRAC6 (IPMI en la LAN) seleccionando **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Red**.

13 Seleccione la opción **Activar IPMI en la LAN** en la sección **Configuración de IPMI**.

14 Haga clic en **Aplicar**.

Uso de la comunicación en serie en la LAN (SOL)

En esta sección se ofrecen diversos métodos para inicializar una sesión de comunicación en serie en la LAN, lo que incluye un programa de Telnet, un cliente SSH, IPMItool y el proxy SOL. El propósito de la función de comunicación en serie en la LAN consiste en redirigir el puerto serie del servidor administrado a través del iDRAC6 a la consola de la estación de administración.

Modelo para dirigir la comunicación en serie en la LAN a través de Telnet o SSH

Cliente de Telnet (puerto 23)/ SSH (puerto 22)←→ Conexión WAN←→ Servidor de iDRAC6

La implementación de la función SOL con base en IPMI a través de SSH/Telnet elimina la necesidad de contar con una utilidad adicional ya que la traducción de comunicación serie a comunicación de red se realiza dentro del iDRAC6. La consola de Telnet o SSH que se utilice debe ser capaz de interpretar y responder a los datos provenientes del puerto serie del servidor administrado. El puerto serie por lo general se conecta a un shell que emula una terminal ANSI o VT100/VT220. La consola serie se envía automáticamente a la consola de Telnet o SSH.

Para iniciar una sesión SOL, conéctese al iDRAC6 a través de SSH/Telnet, lo cual lo lleva a la consola de línea de comandos del iDRAC6. Introduzca `connect` a continuación del símbolo de dólar.

Ver “Instalación de clientes Telnet o SSH” en la página 80 para obtener más información acerca de cómo utilizar clientes Telnet y SSH con el iDRAC6.

Modelo para proxy SOL

Cliente Telnet (puerto 623) ←→ Conexión WAN ←→ Proxy SOL ←→ Servidor del iDRAC6.

Cuando el proxy SOL se comunica con el cliente Telnet en una estación de administración, utiliza el protocolo TCP/IP. No obstante, el proxy SOL se comunica con el iDRAC6 del servidor administrado a través del protocolo RMCP/IPMI/SOL, el cual es un protocolo basado en UDP. Por lo tanto, si la comunicación con el iDRAC6 del sistema administrado desde el proxy SOL se realiza a través de una conexión WAN, es posible que surjan problemas de rendimiento de red. El modelo de uso recomendado es que el proxy SOL y el servidor del iDRAC6 estén en la misma LAN. De esta forma, la estación de administración con el cliente Telnet podrá conectarse al proxy SOL a través de una conexión WAN. En este modelo, el proxy SOL funcionará según se desee.

Modelo para dirigir la comunicación en serie en la LAN a través de IPMItool

IPMItool ←→ Conexión WAN←→ Servidor del iDRAC6

La utilidad SOL basada en IPMI, IPMItool, utiliza el protocolo RMCP+ a través de datagramas UDP con el puerto 623. iDRAC6 requiere que esta conexión RMCP+ esté cifrada. La clave de cifrado (clave KG) debe contener caracteres de valor cero o NULO que puedan configurarse en la interfaz gráfica del usuario de web del iDRAC6 o en la utilidad de configuración del iDRAC6. También es posible borrar la clave de cifrado presionando la tecla de retroceso para que el iDRAC6 proporcione caracteres NULOS, como la clave de cifrado, de manera predeterminada. La ventaja de utilizar RMCP+ es una mejor autentificación, control de integridad de los datos, cifrado y capacidad para varios tipos de carga. Ver “Uso de SOL a través de IPMItool” en la página 215 o el sitio web de IPMItool para obtener más información: **http://ipmitool.sourceforge.net/manpage.html**.

Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6

Los comandos para desconectar una sesión SOL se centran en la utilidad. Puede salir de la utilidad sólo cuando se haya finalizado por completo la sesión SOL. Para desconectar una sesión SOL, finalice la sesión SOL desde la consola de línea de comandos del iDRAC6.

Cuando esté listo para salir de la redirección de SOL, presione <Intro>, <Esc> y después <t> (presione las teclas en secuencia, una tras otra). La sesión SOL se cerrará según corresponda. La secuencia de escape también se muestra en la pantalla al momento de conectarse una sesión SOL. Cuando el servidor administrado está apagado, la sesión SOL demora más tiempo en establecerse.

NOTA: Si la sesión SOL no se cierra correctamente en la utilidad, no habrá más sesiones disponibles. Para resolver esta situación, es necesario finalizar la consola de línea de comandos en la interfaz gráfica del usuario de web en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Sesiones**.

Uso de SOL a través de PuTTY

Para iniciar la comunicación en serie en la LAN desde PuTTY en una estación de administración Windows, siga estos pasos:

NOTA: De ser necesario, puede cambiar el tiempo de espera predeterminado de SSH/Telnet en **Sistema→ Configuración de iDRAC→ Red/Seguridad → Servicios**.

1. Para conectarse al iDRAC6, introduzca lo siguiente en el símbolo del sistema:

   ```
   putty.exe [-ssh | -telnet] <nombre de inicio de sesión>@<dirección_IP_de_iDRAC> <número de puerto>
   ```

NOTA: El número de puerto es opcional. Se requiere únicamente cuando se reasigna el número de puerto.

2. Introduzca lo siguiente en el símbolo del sistema para iniciar SOL:

   ```
   connect
   ```

   Con esto se conectará al puerto serie del servidor administrado. Una vez que se establece una sesión SOL, la consola de línea de comandos del iDRAC6 ya no estará a su disposición. Siga correctamente la secuencia de escape para llegar a la consola de línea de comandos del iDRAC6. Cierre la sesión SOL por medio de la secuencia de comandos que se describe en "Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6" en la página 212 e inicie una nueva.

NOTA: En Windows, si se abre la consola del sistema de administración de emergencia (EMS) inmediatamente después de un inicio de host, la terminal de la consola de administración especial (SAC) puede resultar dañada. Cierre la sesión SOL como se describe en "Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6" en la página 212, cierre la terminal, abra otra terminal e inicie la sesión SOL mediante el mismo comando indicado anteriormente.

Uso de la comunicación en serie en la LAN mediante Telnet con Linux

Para iniciar la comunicación en serie en la LAN por medio de Telnet en una estación de administración con Linux, siga estos pasos:

NOTA: De ser necesario, puede cambiar el tiempo de espera predeterminado de Telnet en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Servicios**.

1. Inicie una ventana de shell.
2. Para conectarse al iDRAC6, introduzca el comando siguiente:

   `telnet <dirección_IP_iDRAC6>`

NOTA: Si cambió el número predeterminado de puerto del servicio de Telnet (puerto 23), agregue el número de puerto al final del comando Telnet.

3. Introduzca lo siguiente en el símbolo del sistema para iniciar SOL:

   `connect`

4. Para salir de una sesión SOL desde Telnet en Linux, presione <Ctrl>+] (mantenga presionada la tecla control y presione la tecla + y el corchete derecho, luego suéltelas). Aparecerá una petición de Telnet. Escriba `quit` para salir de Telnet.

Uso de la comunicación en serie en la LAN mediante OpenSSH con Linux

OpenSSH es una utilidad de código fuente abierto para utilizar el protocolo SSH. Para iniciar la comunicación en serie en la LAN desde OpenSSH en una estación de administración Linux, siga estos pasos:

NOTA: De ser necesario, puede cambiar el tiempo de espera predeterminado de SSH en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Servicios**.

1. Inicie una ventana de shell.
2. Para conectarse al iDRAC6, introduzca el comando siguiente:

   `ssh <dirección_IP_de_iDRAC> -l <nombre de inicio de sesión>`

3. Introduzca lo siguiente en el símbolo del sistema para iniciar SOL:

   `connect`

Con esto se conectará al puerto serie del servidor administrado. Una vez que se establece una sesión SOL, la consola de línea de comandos del iDRAC6 ya no estará a su disposición. Siga correctamente la secuencia de escape para llegar a la consola de línea de comandos del iDRAC6. Cierre la sesión SOL (ver "Desconexión de la sesión SOL en la consola de línea de comandos del iDRAC6" en la página 212 para cerrar una sesión SOL activa).

Uso de SOL a través de IPMItool

El DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) incluye IPMItool, una herramienta que puede instalarse en diversos sistemas operativos. Consulte la *Guía de instalación rápida del software* para obtener información sobre la instalación. Para iniciar la comunicación en serie en la LAN con IPMItool en una estación de administración, siga estos pasos:

NOTA: De ser necesario, puede cambiar el tiempo de espera predeterminado de SOL en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Servicios.**

1. Localice el archivo **IPMItool.exe** en el directorio correspondiente.

   La ruta de acceso predeterminada en el sistema operativo Windows de 32 bits es **C:\Archivos de programa\Dell\SysMgt\bmc**, y en el sistema operativo Windows de 64 bits es **C:\Archivos de programa (x86)\Dell\SysMgt\bmc**.

2. Asegúrese de que la **Clave de cifrado** contenga sólo ceros en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Red→ Configuración de IPMI**.

3. Introduzca el siguiente comando en el indicador de comandos de Windows o en la ventana del símbolo del sistema del shell de Linux para iniciar SOL a través del iDRAC:

   ```
   ipmitool -H <dirección_IP_de_iDRAC> -I lanplus -U
   <nombre de inicio de sesión> -P <contraseña de
   inicio de sesión> sol activate
   ```

   Con esto se conectará al puerto serie del servidor administrado.

4 Para salir de una sesión SOL desde IPMItool, presione <~> y <.> (presione las teclas de tilde y punto en secuencia, una después de la otra). Inténtelo más de una vez, ya que el iDRAC6 puede estar ocupado como para aceptar las teclas. La sesión SOL se cerrará.

NOTA: Si un usuario no finaliza la sesión correctamente, ejecute el siguiente comando para reiniciar el iDRAC. Espere dos minutos hasta que el iDRAC6 se inicie por completo. Para obtener más detalles, consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

```
racadm racreset
```

Ejecución de SOL con el proxy SOL

El proxy de comunicación en serie en la LAN (proxy SOL) es un daemon de Telnet que permite la administración basada en LAN de sistemas remotos con los protocolos de comunicación en serie en la LAN (SOL) e IPMI. Se puede utilizar cualquier aplicación de cliente Telnet estándar, como HyperTerminal en Windows de Microsoft o Telnet en Linux, para acceder a las funciones del daemon. SOL se puede utilizar en el modo ya sea de comando o de menú. El protocolo SOL unido a la consola virtual del BIOS del sistema remoto permite a los administradores ver y cambiar de manera remota la configuración del BIOS del sistema administrado a través de una LAN. También se puede acceder a la consola en serie de Linux y a las interfaces EMS/SAC de Microsoft a través de una LAN mediante SOL.

NOTA: Todas las versiones del sistema operativo Windows incluyen el software de emulación de terminal HyperTerminal. Sin embargo, la versión incluida no proporciona muchas funciones necesarias durante el uso de la consola virtual. En su lugar, puede utilizar cualquier software de emulación de terminal que admita el modo de emulación VT100/VT220 o ANSI. Un ejemplo de un emulador de terminal VT100/VT220 o ANSI completo que admite la consola virtual en el sistema es HyperTerminal Private Edition 6.1 o posterior de Hilgraeve. Además, el uso de la ventana de línea de comandos para ejecutar la consola virtual serie Telnet puede dar lugar a la aparición de caracteres inservibles.

NOTA: Consulte la guía del usuario del sistema para obtener más información acerca de la consola virtual, incluyendo los requerimientos de hardware y software, así como instrucciones para configurar sistemas cliente y host que utilicen la consola virtual.

NOTA: La configuración de HyperTerminal y Telnet debe ser coherente con la configuración del sistema administrado. Por ejemplo, las velocidades en baudios y los modos de terminal deben coincidir.

NOTA: El comando `telnet` de Windows que se ejecuta desde la petición de MS-DOS admite la emulación de terminal ANSI y el BIOS debe estar configurado para la emulación ANSI para que todas las pantallas se muestren correctamente.

Antes de utilizar el proxy SOL

Antes de utilizar el proxy SOL, consulte la *Baseboard Management Controller Utilities User's Guide* (Guía del usuario de las utilidades del controlador de administración de la placa base) para saber cómo configurar las estaciones de administración. De manera predeterminada, las utilidades de administración de BMC están instaladas en el siguiente directorio en los sistemas operativos Windows:

C:\Archivos de programa\Dell\SysMgt\bmc: (sistema operativo de 32 bits)

C:\Archivos de programa (x86)\Dell\SysMgt\bmc: (sistema operativo de 64 bits)

El programa de instalación copia los archivos en las siguientes ubicaciones en los sistemas operativos Linux Enterprise:

/etc/init.d/SOLPROXY.cfg

/etc/solproxy.cfg

/usr/sbin/dsm_bmu_solproxy32d

/usr/sbin/solconfig

/usr/sbin/ipmish

Inicio de sesión del proxy SOL

Para Windows 2003

Para iniciar el servicio proxy SOL en un sistema Windows después de la instalación, puede reiniciar el sistema (el proxy SOL se inicia automáticamente después del reinicio). O bien, puede iniciar el servicio proxy SOL manualmente mediante los siguientes pasos:

1. Haga clic con el botón derecho del mouse en **Mi PC** y haga clic en **Administrar**.

   Aparecerá la ventana **Administración del equipo**.

2 Haga clic en **Servicios y aplicaciones** y luego en **Servicios**.

Los servicios disponibles se muestran a la derecha.

3 Ubique **DSM _BMU_SOLProxy** en la lista de servicios y haga clic con el botón derecho del mouse para iniciar el servicio.

Dependiendo de la consola que utilice, existen distintos pasos para acceder a Proxy SOL. En esta sección, la estación de administración en la que se está ejecutando el proxy SOL se denomina servidor proxy SOL.

En Linux

Proxy SOL se iniciará automáticamente durante el inicio del sistema. Asimismo, puede acceder al directorio **/etc/init.d** y utilizar los siguientes comandos para administrar el servicio Proxy SOL:

```
solproxy status

dsm_bmu_solproxy32d start

dsm_bmu_solproxy32d stop

solproxy restart
```

Uso de Telnet con el proxy SOL

Esta sección parte de la premisa de que el servicio proxy SOL ya está en funcionamiento en la estación de administración.

Para Windows 2003:

1 Abra una ventana del símbolo del sistema en la estación de administración.

2 Introduzca el comando `telnet` en la línea de comandos y escriba `localhost` como dirección IP si el servidor proxy SOL se ejecuta en la misma máquina y el número de puerto que se especificó en la instalación del proxy SOL (el valor predeterminado es `623`). Por ejemplo,

```
telnet localhost 623
```

Para Linux:

1 Abra un shell de Linux en la estación de administración.

2 Introduzca el comando `telnet` y escriba `localhost` como la dirección IP del servidor proxy SOL y el número de puerto que se especificó en la instalación del proxy SOL (el valor predeterminado es `623`). Por ejemplo,

```
telnet localhost 623
```

NOTA: Independientemente de que el sistema operativo host sea Windows o Linux, si el servidor proxy SOL se ejecuta en una máquina diferente a la de la estación de administración, introduzca la dirección IP del servidor proxy SOL en lugar de localhost.

```
telnet <dirección IP del servidor proxy SOL> 623
```

Uso de HyperTerminal con el proxy SOL

1 Desde la estación remota, abra **HyperTerminal.exe**.

2 Elija **TCPIP (Winsock)**.

3 Introduzca la dirección de host `localhost` y el número de puerto `623`.

Conexión al BMC del sistema administrado remoto

Después de iniciar correctamente una sesión de proxy SOL, se le presentarán las siguientes opciones:

```
1. Conectarse al BMC del servidor remoto

2. Configurar la comunicación en serie en la LAN
para el servidor remoto

3. Activar la consola virtual

4. Reiniciar y activar la consola virtual

5. Help (Ayuda)

6. Salir
```

NOTA: Aunque puede haber varias sesiones SOL activas al mismo tiempo, sólo puede haber una sesión de consola virtual activa en un momento dado en un sistema administrado.

NOTA: Para salir de una sesión de SOL activa, utilice la secuencia de caracteres <~><.>. Esta secuencia finaliza SOL y abre el menú de nivel superior.

1 Seleccione la opción 1 en el menú principal.

2 Introduzca la **dirección IP** del iDRAC6 del sistema administrado remoto.

3 Proporcione el **Nombre de usuario** y la **Contraseña** para iDRAC6 en el sistema administrado. El nombre de usuario y la contraseña del iDRAC6 se deben asignar y guardar en el almacenamiento no volátil del iDRAC6.

NOTA: Sólo se permite una sesión de consola virtual SOL con iDRAC6 a la vez.

NOTA: De ser necesario, extienda la duración de la sesión SOL a un número infinito cambiando el valor de **Tiempo de espera** de Telnet a cero en la interfaz gráfica del usuario de web del iDRAC6, en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Servicios**.

4 Proporcione la clave de cifrado de IPMI si ésta se configuró en el iDRAC6.

NOTA: Puede encontrar la clave de cifrado de IPMI en la interfaz gráfica del usuario del iDRAC6 en **Sistema→ Configuración de iDRAC→ Red/Seguridad→ Red→ Configuración de IPMI→ Clave de cifrado**.

NOTA: La clave de cifrado predeterminada de IPMI sólo contiene ceros. Si presiona <Intro> para la opción de cifrado, el iDRAC6 utilizará esta clave de cifrado predeterminada.

5 Seleccione **Configurar la comunicación en serie en la LAN para el servidor remoto** (opción 2) en el menú principal.

Aparecerá el menú de configuración de SOL. De acuerdo con el estado de SOL actual, el contenido del menú de configuración de SOL varía:

- Si SOL ya está activada, los valores actuales se muestran y se presentan tres posibilidades:

```
1. Desactivar la comunicación en serie en la LAN

2. Cambiar la configuración de la comunicación
en serie en la LAN

3. Cancelar
```

- Si SOL está activada, asegúrese de que la velocidad en baudios de SOL concuerde con la del iDRAC6 y que el usuario cuente con el privilegio de administrador.
- Si SOL está desactivada, escriba `Y` para activar esta función o bien `N` para mantenerla en ese estado.

6 Seleccione **Activar la consola virtual** (opción 3) en el menú principal

La consola de texto del sistema administrado remoto se redirige a la estación de administración.

7 Seleccione **Reiniciar y activar la consola virtual** (opción 4) en el menú principal (opcional).

Se confirmará el estado de alimentación del sistema administrado remoto. Si la alimentación está activada, se le pedirá que decida entre un apagado ordenado o forzado.

Después, el estado de la alimentación es supervisado hasta que cambie a **encendido**. La consola virtual comienza y la consola de texto del sistema administrado remoto se redirige a la estación de administración.

Mientras el sistema administrado se reinicia, puede acceder al programa de configuración del sistema del BIOS para ver o configurar los valores del BIOS.

8 Seleccione **Ayuda** (opción 5) en el menú principal para visualizar descripciones detalladas de cada opción.

9 Seleccione **Salir** (opción 6) en el menú principal para finalizar la sesión de Telnet y desconectarse del proxy SOL.

NOTA: Si un usuario no finaliza la sesión correctamente, ejecute el siguiente comando para reiniciar el iDRAC. Espere entre 1 y 2 minutos hasta que el iDRAC6 se inicie por completo. Para obtener más detalles, consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

```
racadm racreset
```

Configuración del sistema operativo

Para configurar sistemas operativos genéricos, realice los pasos pertinentes a su sistema operativo. Esta configuración toma como base las instalaciones predeterminadas de Red Hat Enterprise Linux 5.0, SUSE Linux Enterprise Server 10 SP1 y Windows 2003 Enterprise.

Sistema operativo Linux Enterprise

1 Edite el archivo **/etc/inittab** para activar el control de flujo de hardware y permitir que los usuarios inicien sesión a través de la consola SOL. Agregue la siguiente línea al final de la sección `#Ejecutar gettys en los niveles de ejecución estándares`.

```
7:2345:respawn:/sbin/agetty -h 115200 ttyS0 vt220
```

Ejemplo de **/etc/inittab** original:

```
#
# inittab  Este archivo describe la manera en la que el proceso
           INIT deberá configurar
#          el sistema en un nivel de ejecución determinado.
#

OMITIR esta parte del archivo

# Ejecutar gettys en los niveles de ejecución estándares
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1

# Ejecutar xdm en el nivel de ejecución 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Ejemplo de **/etc/inittab** modificado:

```
#
# inittab    Este archivo describe la manera en la que el proceso
INIT deberá configurar
#            el sistema en un nivel de ejecución determinado.
#

OMITIR esta parte del archivo

# Ejecutar gettys en los niveles de ejecución estándares
1:2345:respawn:/sbin/migetty tty1
2:2345:respawn:/sbin/migetty tty1
```

```
3:2345:respawn:/sbin/migetty tty1
4:2345:respawn:/sbin/migetty tty1
5:2345:respawn:/sbin/migetty tty1
6:2345:respawn:/sbin/migetty tty1
7:2345:respawn:/sbin/agetty -h ttyS0 115200 vt220

# Ejecutar xdm en el nivel de ejecución 5
x:5:respawn:/etc/X11/prefdm -nodaemon
```

2 Edite el archivo **/etc/securetty** para permitir que los usuarios inicien sesión como usuario root a través de la consola SOL. Agregue la siguiente línea después de `consola`:

```
ttyS0
```

Ejemplo de **/etc/securetty** original:

```
consola
vc/1
vc/2
vc/3
vc/4

OMITIR el resto del archivo
```

Ejemplo de **/etc/securetty** modificado:

```
Consola
ttyS0
vc/1
vc/2
vc/3
vc/4

OMITIR el resto del archivo
```

3 Edite el archivo **/boot/grub/grub.conf** o el archivo **/boot/grub/menu.list** para agregar opciones de inicio para SOL:

a Agregue comentarios para las líneas de mensajes gráficos en los sistemas operativos de tipo Unix:

- `splashimage=(had0,0)/grub/splash.xpm.gz` en RHEL 5
- `gfxmenu (hda0,5)/boot/message` en SLES 10

b Agregue la siguiente línea antes de la primera línea `title=` …:

```
# Redirigir inicio de sistema operativo a
través de SOL
```

c Agregue la siguiente entrada a la primera línea `title=` …:

```
Redirección SOL
```

d Agregue el siguiente texto a la línea `kernel/`… del primer `title=` …:

```
console=tty1 console=ttyS0,115200
```

NOTA: **/boot/grub/grub.conf** en Red Hat Enterprise Linux 5 es un vínculo simbólico con **/boot/grub/menu.list**. Puede cambiar la configuración en uno de los dos.

Ejemplo de **/boot/grub/grub.conf** original en RHEL 5:

```
# grub.conf generado por anaconda
#
# Tenga en cuenta que no tiene que volver a ejecutar grub
después de hacer cambios en este
# archivo
# AVISO:  Tiene una partición /boot. Esto significa que
#         todas las rutas de acceso initrd y kernel son
          relativas a /boot/, por ej.
#         root (hd0,0)
#         kernel /vmlinux-version ro root=
/dev/VolGroup00/LogVol00
#         initrd /initrd-version.img
#boot=/dev/sda
```

```
predeterminado=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

título Red Hat Enterprise Linux 5
root (hd0,0)
kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet
initrd /initrd-2.6.18-8.el5.img
```

Ejemplo de **/boot/grub/grub.conf** modificado:

```
# grub.conf generado por anaconda
#
# Tenga en cuenta que no tiene que volver a ejecutar grub
después de hacer cambios en este
# archivo
# AVISO: Tiene una partición /boot. Esto significa que
#        todas las rutas de acceso initrd y kernel son
         relativas a /boot/, por ej.
#        root (hd0,0)
#        kernel /vmlinux-version ro root=
/dev/VolGroup00/LogVol00
#         initrd /initrd-version.img
#boot=/dev/sda
predeterminado=0
timeout=5
#splashimage=(hd0,0)/grub/splash.xpm/gz
hiddenmenu

# Redirigir inicio de sistema operativo a través de SOL
título Red Hat Enterprise Linux 5 redirección SOL
root (hd0,0)
```

```
kernel /vmlinuz-2.6.18-8.el5 ro root=/dev/VolGroup00/LogVol00
rhgb quiet console=tty1 console=ttyS0,115200
initrd /initrd-2.6.18-8.el5.img
```

Ejemplo de **/boot/grub/menu.list** original en SLES 10:

```
#Modificado por YaST2. Última modificación: Sáb 11 oct 21:52:09
UTC 2008
Valor predeterminado 0
Expiración de tiempo 8
gfxmenu (hd0.5)/boot/message

###No cambie este comentario. Identificador YaST2: Nombre
original: linux###
título SUSE Linux Enterprise Server 10 SP1
root (hd0,5)
kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/by-
id/scsi-35000c5000155c resume=/dev/sda5 splash=silent showopts
initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Ejemplo de **/boot/grub/menu.list** modificado en SLES 10:

```
#Modificado por YaST2. Última modificación: Sáb 11 oct 21:52:09
UTC 2008
Valor predeterminado 0
Expiración de tiempo 8
#gfxmenu (hd0.5)/boot/message

###No cambie este comentario. Identificador YaST2: Nombre
original: linux###
título SUSE Linux Enterprise Server 10 SP1 redirección SOL
root (hd0,5)
kernel /boot/vmlinux-2.6.16-46-0.12-bigsmp root=/dev/disk/
by-id/scsi-35000c5000155c resume=/dev/sda5 splash=silent
showopts console=tty1 console=ttyS0,115200
initrd /boot/initrd-2.6.16.46-0.12-bigsmp
```

Windows 2003 Enterprise

1. Determine la identificación de entrada de inicio ingresando bootcfg en la ventana del símbolo del sistema de Windows. Localice la identificación de entrada de inicio de la sección con el nombre de sistema operativo **Windows Server 2003 Enterprise**. Presione <Intro> para ver las opciones de inicialización en la estación de administración.
2. Active EMS en una ventana del símbolo del sistema de Windows ingresando el siguiente comando:

   ```
   bootcfg /EMS ON /PORT COM1 /BAUD 115200
   /ID <Id. de inicialización>
   ```

   NOTA: *<Id. de inicialización>* será la identificación de entrada de inicio del paso 1.
3. Presione <Intro> para verificar que la configuración de la consola EMS surta efecto.

Ejemplo de configuración original de bootcfg:

```
Configuración de cargador de inicio
--------------------
expiración de tiempo: 30
valor predeterminado:
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS

Entradas de inicio
------------
Identificación de entrada de inicio:    1
Nombre del sistema operativo: Windows Server 2003, Enterprise
Ruta de acceso:
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
Opciones de carga de sistema operativo:  /nonexecute=optout
/fastdetect /usepmtimer /redirect
```

Ejemplo de configuración `bootcfg` modificada:

```
Configuración de cargador de inicio
--------------------
expiración de tiempo:  30
valor predeterminado:   multi(0)disk(0)rdisk(0)partition(1)
                        \WINDOWS
redirección:            COM1
redirectbaudrate:       115200

Entradas de inicio
------------
Identificación de entrada de inicio:    1
Nombre de sistema operativo: Windows Server 2003, Enterprise
Ruta de acceso:              multi(0)disk(0)rdisk(0)
                             partition(1)\WINDOWS
Opciones de carga de sistema operativo:  /nonexecute=optout
                                          /fastdetect
                                          /usepmtimer
                                          /redirect
```

10

Uso de la consola virtual de la interfaz gráfica de usuario

Esta sección proporciona información acerca de cómo utilizar la función de consola virtual del iDRAC6.

Descripción general

La función de consola virtual del iDRAC6 permite acceder de manera remota a consolas locales en modo de gráfico o de texto; así, es posible controlar uno o varios sistemas equipados con iDRAC6 desde una única ubicación.

Uso de la consola virtual

La pantalla **Consola virtual** permite administrar el sistema remoto con el teclado, vídeo y mouse en su estación de administración local para controlar los dispositivos correspondientes en un servidor administrado remoto. Esta función se puede usar junto con la función de medios virtuales para realizar instalaciones de software remotas.

Las siguientes reglas se aplican a una sesión de consola virtual:

- Sólo se admite un máximo de dos sesiones simultáneas de consola virtual en cada servidor blade. Ambas sesiones muestran la misma consola de servidor administrado simultáneamente.
- La sesión de consola virtual no se debe ejecutar desde un explorador web del sistema administrado.
- Debe haber disponible un ancho de banda de red de al menos 1 MB/s.

Si un segundo usuario solicita una sesión de consola virtual, el primer usuario recibe una notificación y tiene la opción de rechazar el acceso, permitir sólo vídeo o permitir el acceso compartido completo. El segundo usuario es notificado de que otro usuario tiene el control. El primer usuario debe responder en un lapso de treinta segundos o no se otorgará el acceso al segundo usuario. Cuando hay dos sesiones activas de forma simultánea, el primer usuario ve un mensaje en la esquina superior derecha de la pantalla que identifica al segundo usuario que tiene una sesión activa.

Si ni el primer ni el segundo usuario tienen privilegios de administrador, la finalización de la sección activa del primer usuario finaliza también la sesión del segundo usuario.

Limpiar el caché del explorador

Si tiene algún problema al operar la consola virtual (errores fuera de rango, problemas de sincronización, etc.), limpie la cahé del explorador para quitar/eliminar las versiones anteriores del visor que pueden estar almacenadas en el sistema e inténtelo de nuevo.

Para borrar versiones anteriores del visor de Active-X para IE7, haga lo siguiente:

1. Cierre el Video Viewer y el explorador de Internet Explorer.
2. Abra el explorador de Internet Explorer nuevamente y vaya a **Internet Explorer→ Herramientas→ Administrar complementos** y haga clic en **Activar o desactivar complementos**. Aparece la ventana **Administrar complementos**.
3. Seleccione **Complementos que han sido utilizados por Internet Explorer** del menú desplegable **Mostrar**.
4. Borre **DELL IDRAC AVCView**.

Para limpiar las versiones anteriores del visor Active-X para IE8, haga lo siguiente:

1. Cierre el Video Viewer y el explorador de Internet Explorer.
2. Abra el explorador de Internet Explorer nuevamente y vaya a **Internet Explorer→ Herramientas→ Administrar complementos** y haga clic en **Activar o desactivar complementos**. Aparece la ventana **Administrar complementos**.
3. Desde el menú desplegable **Mostrar**, seleccione **Todos los complementos**.
4. Seleccione **DELL IDRAC AVCView** y haga clic en el enlace **Más información**.
5. Haga clic en **Quitar** desde la ventana **Más información**.
6. Cierre las ventanas **Más información** y **Administrar complementos**.

Para borrar las versiones anteriores del visor de Java en Windows o Linux, haga lo siguiente:

1. En el símbolo del sistema, ejecute `javaws -viewer`

   Aparece el **Visor del caché de Java**.

2. Elimine el elemento titulado *Cliente de consola virtual del iDRAC6* y *JViewer.*

También puede ejecutar la función `javaws -desinstalar` en el símbolo del sistema para quitar todas las aplicaciones de la caché.

Resoluciones de pantalla y velocidades de actualización admitidas

En la Tabla 10-1 se muestra una lista de las resoluciones de pantalla admitidas y las velocidades de actualización correspondientes para una sesión de consola virtual que se ejecuta en el servidor administrado.

Tabla 10-1. Resoluciones de pantalla y velocidades de actualización admitidas

Resolución de pantalla	Velocidad de actualización (Hz)
720 x 400	70
640 x 480	60, 72, 75, 85
800 x 600	60, 70, 72, 75, 85
1024 x 768	60, 70, 72, 75, 85
1280 x 1024	60

Configuración de la estación de administración

Para utilizar la consola virtual en la estación de administración, realice el siguiente procedimiento:

1. Instale y configure un explorador web admitido. Ver “Exploradores web admitidos” en la página 27 y “Configuración de un explorador web admitido” en la página 70.
2. Si usa Firefox o desea usar el visor de Java con Internet Explorer, instale Java Runtime Environment (JRE). Vea la “Instalación de Java Runtime Environment (JRE)” en la página 79.
3. Se recomienda que configure la resolución del monitor en 1280 x 1024 pixeles.

NOTA: Si tiene una sesión de consola virtual activa y hay un monitor de menor resolución conectado con la consola virtual, la resolución de la consola del servidor puede restablecerse si se selecciona el servidor en la consola local. Si el servidor ejecuta un sistema operativo Linux, es posible que la consola X11 no sea visible en el monitor local. Si presiona <Ctrl><Alt><F1> en la consola virtual, se cambiará de Linux a consola de texto.

4 Si está utilizando Internet Explorer para iniciar una sesión de consola virtual con complemento Java, realice lo siguiente:

a En Internet Explorer, vaya a **Herramientas→ Opciones de Internet→ Seguridad→ Sitios de confianza→ Nivel personalizado**.

NOTA: Para sistemas operativos Windows 7 de 64 bits, haga clic en **Herramientas→ Opciones de Internet→ Seguridad→ Internet→ Nivel personalizado**.

b En la pantalla **Configuración de seguridad**, seleccione la opción **Desactivar** para **Preguntar automáticamente si se debe descargar un archivo**.

c Haga clic en **Aceptar** y, a continuación, vuelva a hacer clic en **Aceptar**.

Configuración de la consola virtual y los medios virtuales en la interfaz web del iDRAC6

Para configurar la consola virtual en la interfaz web del iDRAC6, realice los pasos a continuación:

1 Haga clic en **Sistema** y luego en la ficha **Consola/Medios virtuales**.

2 Haga clic en **Configuración** para abrir la pantalla **Configuración**.

3 Configure las propiedades de la consola virtual.En la Tabla 10-2 se describen los valores de la consola virtual.

4 Cuando termine, haga clic en **Aplicar**.

Tabla 10-2. Propiedades de la configuración de la consola virtual

Propiedad	Descripción
Activado	Seleccione esta opción para activar o desactivar la consola virtual. **Seleccionado** indica que la consola virtual está activada. **Deseleccionado** indica que la consola virtual está desactivada. El valor predeterminado es **activado**.
N.º máx. de sesiones	Muestra el número máximo posible de sesiones de consola virtual: **1** ó **2**. Utilice el menú desplegable para cambiar el número máximo permitido de sesiones de consola virtual. El valor predeterminado es **2**.
Sesiones activas	Muestra el número de sesiones de consola activa. Este campo es de sólo lectura.
Número de puerto de teclado y mouse	El número de puerto de red utilizado para conectarse a la opción de teclado/mouse de la consola virtual. Este tráfico siempre está cifrado. Se recomienda cambiar este número si otro programa está usando el puerto predeterminado. El valor predeterminado es **5900**.
Número de puerto de vídeo	El número de puerto de red utilizado para conectar al servicio de pantalla de consola virtual. Se recomienda cambiar este valor si otro programa está utilizando el puerto predeterminado. El valor predeterminado es **5901**.
Cifrado de vídeo activado	**Seleccionado** indica que el cifrado de vídeo está activado. Todo el tráfico que se dirige al puerto de vídeo está cifrado. **Deseleccionado** indica que el cifrado de vídeo está desactivado. El tráfico que va al puerto de vídeo no está cifrado. El valor predeterminado es **Cifrado**. La desactivación del cifrado puede mejorar el rendimiento en las redes más lentas.

Tabla 10-2. Propiedades de la configuración de la consola virtual *(continuación)*

Propiedad	Descripción
Modo de mouse	Elija **Windows** cuando el servidor administrado se esté ejecutando en un sistema operativo Windows. Elija **Linux** si el servidor administrado ejecuta Linux. Elija **USC/Diagnóstico** si el servidor no está funcionando en un sistema operativo Windows o Linux. **NOTA:** Debe seleccionar **USC/Diagnóstico** en HyperV, Dell Diagnostics o USC (Servicios del sistema). El valor predeterminado es **Windows**.
Tipo de complemento de la consola para IE	Cuando utilice Internet Explorer en un sistema operativo Windows, puede elegir entre los siguientes visores: **ActiveX**: el visor *ActiveX para consola virtual* **Java**: el visor *Java para consola virtual* **NOTA:** Según su versión de Internet Explorer, deberá desactivar restricciones de seguridad adicionales (ver "Configuración y uso de medios virtuales" en la página 275"). **NOTA:** Deberá tener instalado Java Runtime Environment en el sistema cliente a fin de utilizar el visor de Java.
Vídeo del servidor local activado	**Seleccionado** indica que la salida al monitor de la consola virtual está activada durante la consola virtual. **Deseleccionado** indica que las tareas que realice con la **consola virtual** no se verán en el monitor local del servidor administrado.

NOTA: Para obtener más información sobre cómo utilizar los medios virtuales con la consola virtual, ver "Configuración y uso de medios virtuales" en la página 275.

Cómo abrir una sesión de consola virtual

Cuando se abre una sesión de consola virtual, la aplicación Dell Virtual Console Viewer (**iDRACView**) se inicia y el escritorio del sistema remoto aparece en el visor. Cuando se utiliza la aplicación **iDRACView** es posible controlar las funciones del mouse y teclado del sistema remoto desde la estación de administración local.

NOTA: Si la consola virtual se inicia desde una estación de administración Windows Vista, se podrían generar mensajes de reinicio en la consola virtual. Para evitarlo, defina los valores de tiempo de espera adecuados en las siguientes ubicaciones: **Panel de contro→ Opciones de energía→ Economizador de energía→ Configuración avanzada→ Disco duro→ Apagar disco duro después de <tiempo_de_espera>** y en el **Panel de control→ Opciones de energía→ Alto rendimiento→ Configuración avanzada→ Disco duro→ Apagar disco duro después de <tiempo_de_espera>**.

Para abrir una sesión de consola virtual en la interfaz web, realice los pasos siguientes:

1. Haga clic en **Sistema→** ficha **Consola/Medios virtuales→ Consola virtual y medios virtuales**.
2. En la pantalla **Consola virtual y medios virtuales**, utilice la información de la Tabla 10-3 para verificar que haya una sesión de consola virtual disponible.

   Si desea reconfigurar los valores de las propiedades que se muestran, ver "Configuración de la consola virtual y los medios virtuales en la interfaz web del iDRAC6" en la página 232.

Tabla 10-3. Información sobre la consola virtual

Propiedad	Descripción
Consola virtual activada	Sí/No
Cifrado de vídeo activado	Sí/No
N.º máx. de sesiones	Muestra el número máximo de sesiones de consola virtual admitidas.
Sesiones activas	Muestra el número actual de sesiones de consola virtual activas.
Modo de mouse	Muestra la aceleración actual del mouse. El **Modo de mouse** se debe elegir según el tipo de sistema operativo instalado en el servidor administrado.

Tabla 10-3. Información sobre la consola virtual *(continuación)*

Propiedad	Descripción
Tipo de complemento de consola	Muestra el tipo de complemento actualmente configurado. **ActiveX**: se iniciará un visor Active-X. El visor Active-X únicamente funciona en Internet Explorer cuando se ejecuta en un sistema operativo Windows. **Java**: se iniciará un visor Java. El visor Java se puede utilizar en cualquier explorador incluso Internet Explorer. Si el cliente se ejecuta en un sistema operativo distinto a Windows, entonces debe utilizar el visor Java. Si está accediendo al iDRAC6 desde Internet Explorer con un sistema operativo Windows, puede elegir el tipo de complemento, ya sea **ActiveX** o **Java**. **NOTA:** Existe la posibilidad de que la consola virtual no se inicie la primera vez para Internet Explorer 8 si se selecciona **Java** como el tipo de complemento.
Vídeo del servidor local activado	**Sí** indica que la salida al monitor de la consola virtual está activada durante la consola virtual. **No** indica que las tareas que realice con la **consola virtual** no se verán en el monitor local del servidor administrado.

NOTA: Para obtener información sobre cómo usar los medios virtuales con la consola virtual, ver "Configuración y uso de medios virtuales" en la página 275.

3 Si hay una sesión de consola virtual disponible, haga clic en **Iniciar Consola virtual**.

NOTA: Pueden aparecer varias ventanas de mensaje después de iniciar la aplicación. Para evitar el acceso no autorizado a la aplicación, navegue a través de estas ventanas de mensajes dentro de los tres minutos. De lo contrario, se le pedirá iniciar la aplicación nuevamente.

NOTA: Si una o varias ventanas de **Alerta de seguridad** aparecen en los pasos siguientes, lea la información contenida en la ventana y haga clic en **Sí** para continuar.

La estación de administración se conecta al iDRAC6 y el escritorio del sistema remoto aparece en **iDRACView**.

4 Aparecen dos punteros de mouse en la ventana del visor: Uno para el sistema remoto y otro para el sistema local. Usted deberá sincronizarlos de manera que el apuntador remoto siga al apuntador local. Vea la "Sincronización de los apuntadores del mouse" en la página 242.

Vista previa de la consola virtual

Antes de iniciar la consola virtual, puede ver una vista previa del estado de la consola virtual en la página **Sistema→ Propiedades→ Resumen del sistema**. La sección **Vista previa de la consola virtual** muestra una imagen del estado de la consola virtual. La imagen se actualiza cada 30 segundos.

NOTA: La imagen de la consola virtual está disponible únicamente si se ha activado la consola virtual.

Tabla 10-4 ofrece información acerca de las opciones disponibles.

Tabla 10-4. Opciones de Vista previa de la consola virtual

Opción	Descripción
Iniciar	Haga clic en este botón para iniciar la consola virtual. Si sólo está activado Medios virtuales, al hacer clic en este vínculo se inician directamente los medios virtuales. Este botón está desactivado si no se tienen privilegios para consola virtual o si tanto la consola virtual como los medios virtuales están desactivados.
Valor	Haga clic en este vínculo para ver o editar los valores de configuración de la consola virtual en la página **Configuración de consola/medios virtuales**.
Refresh (Actualizar)	Haga clic en este botón para actualizar la imagen de la consola virtual que se muestra.

Uso de Video Viewer

Video Viewer proporciona una interfaz de usuario entre la estación de administración y el servidor administrado que le permite ver la pantalla de escritorio del servidor administrado y controlar las funciones de mouse y teclado desde la estación de administración. Cuando usted se conecta al sistema remoto, Video Viewer se inicia en otra ventana.

NOTA: La barra de título de la consola virtual muestra el nombre DNS o la dirección IP del iDRAC al que se conecta desde la estación de administración. Si el iDRAC no tiene un nombre DNS, se muestra la dirección IP. El formato es: `<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>`

Video Viewer proporciona varios ajustes de control, por ejemplo, modo de color, sincronización del mouse, instantáneas, macros de teclado, acciones de alimentación y acceso a los medios virtuales. Haga clic en **Ayuda** para obtener más información sobre estas funciones.

Si al iniciar una sesión de consola virtual aparece Video Viewer, es posible que se deba ajustar el modo de color y sincronizar los punteros del mouse.

La Tabla 10-5 describe las opciones del menú disponibles en el visor.

Tabla 10-5. Selecciones de la barra de menú del visor

Elemento del menú	Elemento	Descripción
Video	Pause	Pausa la consola virtual temporalmente.
	Reanudar	Reanuda la consola virtual.
	Refresh (Actualizar)	Vuelve a trazar la imagen de la pantalla del visor.
	Capturar la pantalla actual	Captura la pantalla del sistema remoto actual en un archivo **.bmp**. Aparece un cuadro de diálogo que permite guardar el archivo en un lugar determinado.
	Pantalla completa	Para expandir el Video Viewer a modo de pantalla completa, haga clic en la esquina superior derecha del visor para obtener la pantalla completa.
	Salir	Cuando haya terminado de utilizar la consola y haya cerrado la sesión (mediante el procedimiento de desconexión del sistema remoto), seleccione **Salir** desde el menú **Vídeo** para cerrar la ventana del **Video Viewer.**

Tabla 10-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Keyboard (Teclado)	Mantener presionada la tecla Alt derecha	Seleccione este elemento antes presionar las teclas que desea combinar con la tecla <Alt> derecha.
	Mantener presionada la tecla Alt izquierda	Seleccione este elemento antes de presionar las teclas que desea combinar con la tecla <Alt> izquierda.
	Tecla Windows izquierda	Seleccione **Mantener presionado** antes de teclear los caracteres que desea combinar con la tecla Windows izquierda. Seleccione **Presionar y soltar** para enviar una pulsación de la tecla Windows izquierda.
	Tecla Windows derecha	Seleccione **Mantener presionado** antes de teclear los caracteres que desea combinar con la tecla Windows derecha. Seleccione **Presionar y soltar** para enviar una pulsación de la tecla Windows derecha.

Tabla 10-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
	Macros	Al seleccionar una macro o presionar la tecla aceleradora especificada para la macro, la acción se ejecuta en el sistema remoto. Video Viewer ofrece las macros siguientes: • Alt+Ctrl+Supr • Alt+Tab • Alt+Esc • Ctrl+Esc • Alt+Espacio • Alt+Intro • Alt+Guión • Alt+F4 • ImprPant • Alt+ImprPant • F1 • Pause • Alt+M • Alt+D • Alt+ImprPant+M • Alt+ImprPant+P
	Paso a través de teclado	El modo de paso a través de teclado permite redirigir todas las funciones del teclado en el cliente al servidor.
Mouse	**Sincronizar el cursor**	Sincroniza el cursor de modo que el mouse del cliente se redirija al del servidor.
	Ocultar cursor local	Sólo aparecerá el cursor de la consola virtual. Se recomienda esta configuración al ejecutar el USC en una consola virtual.

Tabla 10-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Opciones	Modo de color	Permite seleccionar la profundidad del color para mejorar el rendimiento en la red. Por ejemplo, si va a instalar software a partir de soportes virtuales, puede seleccionar la profundidad de color más baja para que el visor de la consola virtual utilice menos ancho de banda y se destine mayor ancho de banda a la transferencia de datos de los soportes. El modo de color puede definirse en color de 15 bits y 7 bits.
Alimentación	Encender el sistema	Enciende el sistema.
	Apagar el sistema	Apaga el sistema.
	Apagado ordenado	Apaga el sistema.
	Restablecer el sistema (reinicio mediante sistema operativo)	Reinicia el sistema sin apagarlo.
	Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)	Apaga y luego reinicia el sistema.

Tabla 10-5. Selecciones de la barra de menú del visor *(continuación)*

Elemento del menú	Elemento	Descripción
Soportes	Asistente de medios virtuales	El menú **Medios** ofrece acceso al Asistente de medios virtuales, el cual permite redirigir a un dispositivo o imagen, por ejemplo: • Unidad de disco flexible • CD • DVD • Imagen en formato ISO • Unidad flash USB Para obtener información sobre la función de medios virtuales, ver "Configuración y uso de medios virtuales" en la página 275. Se debe mantener activa la ventana del visor de la consola virtual cuando se utilizan los medios virtuales.
Help (Ayuda)	Acerca de iDRACView	Aparece la versión de iDRACView.

Sincronización de los apuntadores del mouse

Cuando se conecta a un sistema Dell PowerEdge remoto utilizando la consola virtual, la velocidad de aceleración del mouse en el sistema remoto podría no corresponder con la del apuntador del mouse en la estación de administración, ocasionando la aparición de dos apuntadores del mouse en la ventana de Video Viewer.

Para sincronizar los apuntadores del mouse, haga clic en **Mouse→ Sincronizar el cursor** o presione <Alt><M>.

La opción del menú Sincronizar el cursor es un interruptor. Asegúrese que al lado de la opción del menú haya una marca; esto indica que la sincronización del mouse está activada.

Cuando se utiliza Red Hat Enterprise Linux o Novell SUSE Linux, asegúrese de configurar el modo de mouse para Linux antes de iniciar el visor. Ver "Configuración de la consola virtual y los medios virtuales en la interfaz web del iDRAC6" en la página 232 para obtener ayuda con la configuración. La configuración predeterminada del mouse del sistema operativo se utiliza para controlar la flecha del mouse en la pantalla de la **consola virtual** del iDRAC6.

Cuando se visualizan dos cursores del mouse en la pantalla de la consola virtual del cliente, se indica que el sistema operativo del servidor admite el Posicionamiento relativo. Es normal en sistemas operativos Linux o en el Universal Server Configurator de Dell (USC). Si la configuración de aceleración del mouse del servidor es diferente a la configuración de aceleración del mouse en el cliente de la consola virtual se producirá la aparición de dos cursores de mouse. Para solucionar este problema, puede cambiar a un sólo cursor seleccionando Cursor sencillo del menú Herramientas (en la pantalla Consola virtual) o intentar hacer coincidir la aceleración del mouse en el servidor y el cliente.

NOTA: Esta situación no se produce en servidores que ejecutan los sistemas operativos Windows ya que éstos admiten el Posicionamiento absoluto.

Cuando se utilice la Consola virtual iDRAC para conectar a un servidor administrado con un sistema operativo de distribución de Linux recientemente instalado, puede experimentar problemas de sincronización del mouse. Es posible que esta situación se deba a la función Aceleración del puntero de predicción del escritorio GNOME. Se debe desactivar esta función para establecer una correcta sincronización del mouse en la Consola virtual de iDRAC. Para desactivar la función Aceleración del puntero de predicción, en la sección del mouse del archivo **/etc/X11/xorg.conf**, agregue:

`Opción "AccelerationScheme" "lightweight".`

Si se siguen produciendo problemas de sincronización, realice el siguiente cambio adicional en el archivo **<user_home>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml**:

Cambie los valores de `motion_threshold` y `motion_acceleration` a `-1`.

Desactivación o activación de la consola local

Es posible configurar el iDRAC6 para rechazar conexiones de consola virtual por medio de la interfaz web del iDRAC6. Cuando aparezca la consola local, se mostrará un punto de estado amarillo en la lista de servidores (en la consola local) para indicar que se ha bloqueado la consola en iDRAC6. Cuando la consola local está activada, el punto de estado es verde.

Si desea tener acceso exclusivo a la consola del servidor administrado, deberá desactivar la consola local *y* volver a configurar el **Número máximo de sesiones** a `1` en la **pantalla de** la consola virtual.

NOTA: Si desactiva (apaga) el vídeo local en el servidor, se desactivarán el monitor, teclado y mouse que están conectados a la consola virtual.

Para desactivar o activar la consola local, realice el procedimiento siguiente:

1. En la estación de administración, abra un explorador web admitido e inicie sesión en el iDRAC6. Ver "Acceso a la interfaz web" en la página 90 para obtener más información.
2. Haga clic en **Sistema**, haga clic en la ficha **Consola/Medios virtuales** y después haga clic en **Configuración**.
3. Si desea desactivar (apagar) el vídeo local en el servidor, en la pantalla **Configuración** deseleccione la casilla **Vídeo del servidor local activado** y después haga clic en **Aplicar**. El valor predeterminado es **Activado** (seleccionado).
4. Si desea activar (encender) el vídeo local en el servidor, en la pantalla **Configuración** seleccione la casilla **Vídeo del servidor local activado** y después haga clic en **Aplicar**.

La pantalla **Consola virtual** muestra el estado del vídeo del servidor local.

Inicio de la consola virtual y de los medios virtuales de manera remota

Puede iniciar la consola virtual o los medios virtuales ingresando un único URL en un explorador admitido, en lugar de iniciarlo desde la interfaz gráfica del usuario de web del iDRAC6. Dependiendo de la configuración de su sistema, deberá pasar por el proceso de autentificación manual (página de inicio de sesión) o será dirigido automáticamente al visor de la consola virtual o los medios virtuales (iDRACView).

NOTA: Internet Explorer admite el inicio de sesión local, con Active Directory (AD), tarjeta inteligente (SC) e inicio de sesión único (SSO). Firefox admite inicios de sesión SSO, locales y AD.

Formato de URL

Si introduce el vínculo **https://<ip_del_idrac6>/consola** en el explorador, es probable que deba realizar el proceso de inicio de sesión manual normal, dependiendo de la configuración de inicio de sesión. Si la opción SSO no está activada, y Local, AD o SC sí están, aparece la página de inicio de sesión correspondiente. Si la sesión se inicia correctamente, no se inicia la vista de consola virtual o de medios virtuales. En su lugar, será redireccionado a la página de inicio de la interfaz gráfica de usuario del iDRAC6.

NOTA: El URL utilizado para iniciar el iDRACView distingue entre mayúsculas y minúsculas y deberá ser escrito en minúsculas.

Situaciones de error habituales

Tabla 10-6 enumera las situaciones de errores generales, las razones de estos errores y el comportamiento del iDRAC6.

Tabla 10-6. Situaciones de error

Situaciones de error	Motivo	Comportamiento
Falló el inicio de sesión	Ingresó un nombre de usuario no válido o una contraseña incorrecta.	El mismo comportamiento cuando se especifica *https://<ip>* y falla el inicio de sesión.
Privilegios insuficientes	No cuenta con los privilegios de consola virtual y soportes virtuales.	iDRACView no se inicia y es redireccionado a la página de la interfaz gráfica de usuario para la configuración de la consola/medios virtuales.
Consola virtual desactivada	La consola virtual está desactivada en su sistema.	iDRACView no se inicia y es redireccionado a la página de la interfaz gráfica de usuario para la configuración de la consola/medios virtuales.
Se detectaron parámetros de URL desconocidos	El URL introducido incluye parámetros no definidos.	Aparece el mensaje No se encontró la página (404).

Preguntas frecuentes

La Tabla 10-7 contiene las preguntas y respuestas frecuentes.

Tabla 10-7. Uso de la consola virtual: preguntas frecuentes

Pregunta	Respuesta
La consola virtual no cierra la sesión cuando se desconecta la interfaz gráfica de usuario web fuera de banda.	Las sesiones de la consola virtual y los medios virtuales permanecen activas incluso cuando la sesión de web se desconecta. Cierre las aplicaciones del visor de medios virtuales y de la consola virtual para desconectarse de la sesión correspondiente.
¿Se puede iniciar una nueva sesión de vídeo de consola remota cuando el vídeo local del servidor está apagado?	Sí.
¿Por qué tarda 15 segundos apagar el vídeo local del servidor después de solicitar la desactivación del vídeo local?	Para que el usuario local tenga la oportunidad de realizar alguna acción antes de que el vídeo se apague.
¿Hay algún retraso al encender el vídeo local?	No, una vez que el iDRAC6 recibe la solicitud de **encendido** del vídeo local, este último se enciende instantáneamente.
¿El usuario local también puede apagar el vídeo?	Sí, el usuario local puede utilizar la CLI de RACADM local para apagar el vídeo.
¿El usuario local también puede encender el vídeo?	No. Después de que la consola local se desactive, el teclado y el mouse del usuario local se desactivarán y no podrán hacer cambios de configuración.
¿La desactivación del vídeo local también desactiva el teclado y el mouse locales?	Sí.
¿La desactivación de la consola local desactivará el vídeo en la sesión de consola remota?	No, la activación o desactivación del vídeo local es independiente de la sesión de consola remota.
¿Cuáles son los privilegios necesarios para que un usuario del iDRAC6 active o desactive el vídeo del servidor local?	Cualquier usuario con privilegios de configuración del iDRAC6 puede activar o desactivar la consola local.

Tabla 10-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Cómo se puede ver el estado actual del vídeo del servidor local?	El estado se muestra en la pantalla **Consola virtual y medios virtuales** de la interfaz web del iDRAC6. El comando `racadm getconfig -g cfgRacTuning` de la interfaz de línea de comandos de RACADM muestra el estado en el objeto **cfgRacTuneLocalServerVideo**. Este comando de racadm se puede ejecutar desde Telnet/SSH o una sesión remota al iDRAC6. El comando de RACADM remoto es: `racadm -r <idracip> -u <user> -p <password> getconfig -g cfgRacTuning` El estado también se muestra en la pantalla de OSCAR de consola virtual. Cuando la consola local está activada, aparece un indicador de estado verde al lado del nombre del servidor. Cuando está desactivada, un punto amarillo indica que el iDRAC6 ha bloqueado la consola local.
No puedo ver la parte inferior de la pantalla del sistema en la ventana de la consola virtual.	Compruebe que la resolución del monitor de la estación de administración sea de 1280 x 1024.
La ventana de la consola no es legible.	El visor de la consola virtual en Linux requiere de un conjunto de caracteres UTF-8. Revise la configuración regional y, de ser necesario, restablezca el conjunto de caracteres. Para obtener más información, ver "Cómo establecer la configuración regional en Linux" en la página 75.
¿Por qué aparece una pantalla en blanco en el servidor administrado al cargar el sistema operativo Windows 2000?	El servidor administrado no tiene el archivo controlador correcto de vídeo ATI. Actualice el controlador de vídeo.

Tabla 10-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Por qué el mouse no se sincroniza en DOS cuando se ejecuta la consola virtual?	El BIOS de Dell emula el controlador de mouse como mouse PS/2. Debido al diseño, el mouse PS/2 utiliza la posición relativa para el apuntador del mouse, lo que ocasiona un retraso en la sincronización. El iDRAC6 tiene un controlador de mouse USB, que permite la posición absoluta y un seguimiento más preciso del apuntador del mouse. Aun cuando el iDRAC6 pasara la posición absoluta del mouse USB al BIOS de Dell, la emulación del BIOS lo convertiría nuevamente a la posición relativa y el comportamiento seguiría siendo el mismo. Para solucionar este problema, establezca el modo de mouse en **USC/Diagnóstico** en la pantalla **Configuración**.
¿Por qué no se sincroniza el mouse en la consola de texto de Linux (ya sea en Dell Unified Server Configurator (USC), Dell Lifecycle Controller (LC) o en Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE)?	La consola virtual necesita el controlador de mouse USB, pero éste sólo está disponible en el sistema operativo X-Window.
Aún tengo problemas con la sincronización del mouse.	Compruebe que el mouse adecuado esté seleccionado para el sistema operativo antes de iniciar una sesión de consola virtual. Compruebe que **Sincronizar el mouse** esté seleccionado en el menú **Mouse**. Presione <Alt><M> o seleccione **Mouse→ Sincronizar el mouse** para activar/desactivar la sincronización del mouse. Cuando la sincronización está activada, aparecerá una marca junto a la selección en el menú **Mouse**.

Tabla 10-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Por qué no puedo usar un teclado o un mouse mientras instalo un sistema operativo Microsoft de manera remota mediante la consola virtual del iDRAC6?	Cuando se instala de manera remota un sistema operativo Microsoft admitido en un sistema con la consola virtual activada en el BIOS, aparece un mensaje de conexión de EMS que pide que se seleccione **Aceptar** para poder continuar. No se puede usar el mouse para seleccionar **Aceptar** de manera remota. Se debe seleccionar **Aceptar** en el sistema local o reiniciar el servidor administrado de manera remota, volver a instalar y luego desactivar la consola virtual en el BIOS. Microsoft genera este mensaje para avisar al usuario que la consola virtual está activada. Para asegurar que este mensaje no aparezca, siempre desactive la consola virtual en el BIOS antes de instalar un sistema operativo de manera remota.
¿Por qué el indicador de Bloq Num de mi estación de administración no muestra el estado de Bloq Num en el servidor remoto?	Cuando se accede por medio del iDRAC6, el indicador Bloq Num de la estación de administración no necesariamente coincide con el estado del Bloq Num del servidor remoto. El estado de Bloq Num depende de la configuración del servidor remoto cuando la sesión remota está conectada, independientemente del estado de Bloq Num en la estación de administración.
¿Por qué aparecen varias ventanas del visor de sesión cuándo establezco una sesión de consola virtual desde el host local?	Está configurando una sesión de consola virtual desde el sistema local. Esto no se permite.
Si estoy ejecutando una sesión de consola virtual y un usuario local accede al servidor administrado, ¿recibiré un mensaje de advertencia?	No. Si un usuario local tiene acceso al sistema, usted y él tendrán el control del sistema.

Tabla 10-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Cuánto ancho de banda necesito para ejecutar una sesión de consola virtual?	Se recomienda utilizar una conexión de 5 MB/seg. para lograr un buen rendimiento. Se requiere una conexión de 1 MB/s para un rendimiento mínimo.
¿Cuáles son los requisitos mínimos del sistema para que mi estación de administración ejecute la consola virtual?	La estación de administración requiere un procesador Intel Pentium III a 500 MHz con un mínimo de 256 MB de RAM.
Después de iniciar la consola virtual, sólo puedo utilizar el mouse en la consola virtual y no en mi sistema local. ¿Por qué es esto y que debo hacer para poder utilizar el mouse en la consola virtual y en mi sistema local?	Esto ocurre si el **Modo mouse** se configura en **USC/Diags**. Presione la tecla de acceso directo <Alt><M> para utilizar el mouse en su sistema local. Presione nuevamente <Alt><M> para utilizar el mouse en la consola virtual.
Cuando inicio la GUI y la Consola virtual en iDRAC desde la interfaz de web de CMC, ¿Por qué expira mi sesión GUI?	Cuando se inicia la consola virtual en iDRAC desde la interfaz web de CMC, se abre un menú emergente para iniciar la consola virtual. El menú emergente se cierra en breve tras la apertura de la consola virtual. Cuando se inicia la GUI y la consola virtual en el mismo sistema iDRAC de una estación de administración, expirará la sesión de la GUI de iDRAC si la GUI se inicia antes de que se cierre el menú emergente. Si la GUI de iDRAC se inicia desde la interfaz web de CMC después de que el menú emergente con la consola virtual se cierre, no se producirá este problema.

Tabla 10-7. Uso de la consola virtual: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
La tecla SysRq de Linux no funciona con Internet Explorer. ¿Por qué?	El comportamiento de la tecla SysRq de Linux es diferente cuando se utiliza la consola virtual desde Internet Explorer. Para enviar la tecla SysRq, se debe presionar y soltar la tecla **Impirmir pantalla** mientras se mantienen pulsadas las teclas **Ctrl** y **Alt**. A continuación se muestran los pasos a seguir para enviar la tecla SysRq a un servidor Linux remoto a través de iDRAC, al utilizar Internet Explorer: **1** Active la función de tecla mágica del servidor Linux remoto. Puede utilizar el siguiente comando para activarla en el terminal de Linux. `echo 1 > /proc/sys/kernel/sysrq` **2** Active el modo Paso a través del visor de Active X. **3** Presione **Ctrl** + **Alt** + **Imprimir pantalla**. **4** Suelte solamente la tecla **Imprimir pantalla**. **5** Presione **Imprimir pantalla** + **Ctrl** + **Alt**. **NOTA:** La función SysRq no es actualmente compatible con Internet Explorer y Java.

11

Configuración de la tarjeta vFlash SD y administración de las particiones vFlash

La tarjeta vFlash SD es una tarjeta Secure Digital (SD) que se conecta en la ranura para tarjeta opcional del iDRAC6 Enterprise ubicada en la esquina posterior del sistema. La tarjeta proporciona espacio de almacenamiento que actúa como un dispositivo de memoria USB Flash común. Es el lugar de almacenamiento de las particiones definidas por el usuario que se pueden configurar para exponerlas al sistema como dispositivos USB y también usarlas para crear un dispositivo USB de inicio. Según el modo de emulación seleccionado, las particiones se presentarán al sistema como una unidad de disco flexible, un disco duro o una unidad CD/DVD. Cualquiera de éstos puede definirse como dispositivo de inicio.

Se admiten tarjetas vFlash SD y tarjetas SD estándar. Una *tarjeta vFlash SD* es una tarjeta que admite las nuevas funciones vFlash mejoradas. Una *tarjeta SD estándar* es una tarjeta SD normal genérica que sólo admite algunas funciones vFlash.

Con una tarjeta vFlash SD se pueden crear hasta 16 particiones. Se puede asignar un nombre de etiqueta a la partición al crearla, y es posible realizar diversas operaciones para administrar y utilizar las particiones. Una tarjeta vFlash SD puede ser de cualquier tamaño hasta 8 GB. Cada partición puede tener hasta 4 GB.

Una tarjeta SD estándar puede ser de cualquier tamaño, pero sólo admite una partición. El tamaño de la partición está limitado a 256 MB. El nombre de la etiqueta de la partición es VFLASH de forma predeterminada.

NOTA: Asegúrese de insertar solamente una tarjeta vFlash SD o una tarjeta SD estándar en la ranura para tarjeta de iDRAC6 Enterprise. Si inserta una tarjeta de cualquier otro formato (por ejemplo, una tarjeta multimedia [MMC]), aparece el siguiente mensaje de error al inicializar la tarjeta: *Se ha producido un error al inicializar la tarjeta SD.*

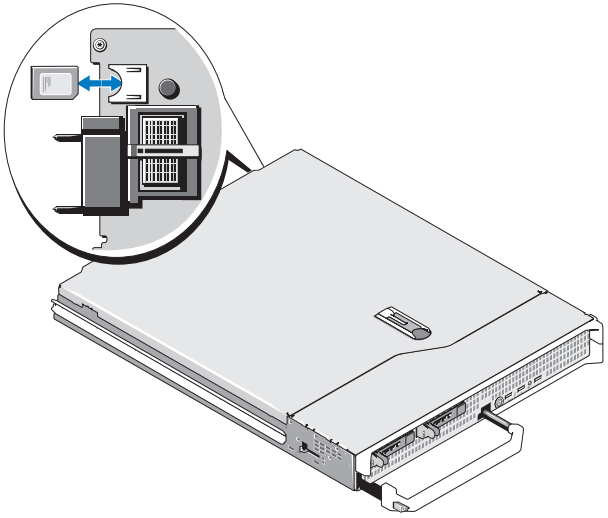
Si es un administrador, puede realizar todas las operaciones en las particiones vFlash. Si no lo es, debe tener privilegios para acceder a los medios virtuales para poder crear, eliminar, formatear, conectar, desconectar o copiar el contenido de la partición.

NOTA: Sólo es posible realizar una única operación vFlash a la vez. Se debe completar la primera operación antes de realizar otra operación vFlash. Por ejemplo: Si comienza una operación de creación a partir de imagen por medio de RACADM, no puede realizar una operación de creación, descarga o formateo mediante la utilización de RACADM o de la interfaz gráfica de usuario. Debe esperar hasta completar la operación antes de realizar la siguiente operación vFlash.

Instalación de una tarjeta SD estándar o vFlash

1. Extraiga el módulo de alta densidad del chasis.
2. Localice la ranura para tarjetas multimedios vFlash en la esquina posterior del sistema.

   NOTA: No es necesario extraer la cubierta del módulo de alta densidad para instalar o extraer la tarjeta.



3. Con la etiqueta hacia arriba, inserte el extremo con los contactos de la tarjeta SD en la ranura para tarjetas del módulo.

   NOTA: La ranura está diseñada para que la tarjeta se inserte correctamente.

4 Presione hacia dentro la tarjeta para encajarla en la ranura.

5 Vuelva a instalar el módulo en el chasis.

Extracción de una tarjeta SD estándar o vFlash

Para extraer la tarjeta SD estándar o vFlash, presione hacia dentro la tarjeta para soltarla y extráigala de la ranura.

Configuración de la tarjeta SD estándar o vFlash mediante la interfaz web del iDRAC6

Después de instalar la tarjeta SD estándar o vFlash, puede ver sus propiedades, activar o desactivar vFlash e inicializar la tarjeta. La tarjeta debe estar activada para poder administrar las particiones. Cuando la tarjeta está desactivada, sólo es posible ver sus propiedades. La operación de inicialización elimina las particiones existentes y restablece la tarjeta.

NOTA: Debe tener permiso para configurar el iDRAC para activar o desactivar vFlash, o para poder inicializar la tarjeta.

Si la tarjeta no se encuentra en la ranura para tarjetas del iDRAC6 Enterprise del sistema, aparece el mensaje de error siguiente.

```
No se detectó la tarjeta SD. Inserte una tarjeta SD de
256 MB o de tamaño o superior.
```

Para ver y configurar la tarjeta SD estándar o vFlash:

1 Abra un explorador web compatible e inicie sesión en la interfaz web del iDRAC6.

2 Seleccione **Sistema** en el árbol del sistema.

3 Haga clic en la ficha **vFlash**. Aparece la página **Propiedades de la tarjeta SD**.

En la Tabla 11-1 se enumeran las propiedades mostradas para la tarjeta SD.

Tabla 11-1. Propiedades de la tarjeta SD

Atributo	Descripción
Name (Nombre)	Muestra el nombre de la tarjeta instalada en la ranura para tarjetas del iDRAC6 Enterprise. Si la tarjeta admite las nuevas funciones vFlash mejoradas, muestra *tarjeta vFlash SD*. Si admite ciertas funciones vFlash, muestra *tarjeta SD*.
Tamaño	Muestra el tamaño de la tarjeta en gigabytes (GB).
Available Space	Muestra el espacio no utilizado de la tarjeta SD en MB. Este espacio está disponible para crear más particiones en la tarjeta vFlash SD. Si la tarjeta SD insertada está sin inicializar, el espacio disponible muestra que la tarjeta está sin inicializar.
Protegida contra escritura	Muestra si la tarjeta está protegida contra escritura o no.
Condición	Muestra la condición general de la tarjeta SD. Ésta puede ser: • En buen estado • Aviso • Critical (Crítico) Si es un aviso, reinicialice la tarjeta. Si es crítico, reinstale y reinicialice la tarjeta.
Activar vFlash	Seleccione la casilla de marcación para administrar la partición vFlash de la tarjeta. Quite la marca de la casilla de marcación para desactivar la administración de la partición vFlash.

4 Haga clic en **Aplicar** para activar o desactivar la administración de la partición vFlash en la tarjeta.

Si hay alguna partición vFlash conectada, no es posible desactivar vFlash y aparece un mensaje de error.

NOTA: Si se desactiva vFlash, sólo se pueden ver las propiedades de la tarjeta SD y no se pueden realizar otras operaciones vFlash, como crear particiones (vacías y con un archivo de imagen), administrar particiones, formatear particiones y descargar contenido para una partición.

5 Haga clic en **Inicializar**. Se eliminan todas las particiones existentes y la tarjeta se restablece. Aparece un mensaje de confirmación.

6 Haga clic en **OK** (Aceptar). Luego de completar la operación de inicialización, aparece un mensaje de ejecución satisfactoria.

NOTA: Inicializar sólo está disponible si se selecciona la opción **Activar vFlash**.

Si hay alguna partición vFlash conectada, la operación de inicialización falla y aparece un mensaje de error.

Si hace clic en cualquier opción de las páginas Flash mientras una aplicación como el proveedor WSMAN, la utilidad de configuración del iDRAC6, o RACADM está utilizando vFlash o si navega a alguna otra página en la interfaz gráfica de usuario, iDRAC6 puede mostrar el mensaje siguiente.

```
La tarjeta SD no está disponible temporalmente. Para
volver a intentar, haga clic en Actualizar.
```

Configuración de una tarjeta SD estándar o vFlash utilizando racadm

Se puede ver y configurar la tarjeta SD estándar o vFlash utilizando comandos de racadm desde una consola local, remota o Telnet/SSH.

NOTA: Debe tener permiso para configurar el iDRAC para activar o desactivar vFlash, y para inicializar la tarjeta.

Cómo mostrar las propiedades de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca el siguiente comando:

```
racadm getconfig -g cfgvFlashSD
```

Aparecen las siguientes propiedades de sólo lectura:

- `cfgvFlashSDSize`
- `cfgvFlashSDLicense`
- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`

Activación o desactivación de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca el siguiente comando:

- Para activar una tarjeta SD estándar o vFlash:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
  ```

- Para desactivar una tarjeta SD estándar o vFlash:

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
  ```

NOTA: El comando racadm sólo funciona si hay una tarjeta SD estándar o vFlash presente. Si no hay una tarjeta presente, se muestra el siguiente mensaje: *ERROR: Tarjeta SD ausente.*

Inicialización de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca el siguiente comando:

```
racadm  vflashsd  initialize
```

Se eliminan todas las particiones existentes y la tarjeta se restablece.

Obtención del último estado de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión y escriba el comando siguiente para obtener el estado del último comando enviado a la tarjeta SD estándar o vFlash:

```
racadm vFlashsd status
```

Restablecimiento de la tarjeta SD estándar o vFlash

Abra una consola telnet/SSH/serie en el servidor, inicie sesión e introduzca:

```
racadm vflashsd initialize
```

Para obtener más información sobre `vflashsd`, consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC6 y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

NOTA: El comando `racadm vmkey reset` se ha descartado a partir de la versión 1.5. La funcionalidad de este comando está cubierta ahora por `vflashsd initialize`. Aunque la ejecución del comando `vmkey reset` será satisfactoria, se recomienda utilizar el comando `vflashsd initialize`. Para obtener más información, consulte "Inicialización de la tarjeta SD estándar o vFlash" en la página 258.

Administración de las particiones vFlash mediante la interfaz web del iDRAC6

Puede realizar las siguientes tareas:

- Crear una partición vacía
- Crear una partición utilizando un archivo de imagen
- Formatear una partición
- Ver las particiones disponibles
- Modificar una partición
- Adjuntar/separar una partición
- Eliminar las particiones existentes
- Descargar el contenido de una partición
- Iniciar una partición

Creación de una partición vacía

Una partición vacía es similar a una memoria USB vacía. Se pueden crear particiones vacías en una tarjeta SD estándar o vFlash. Se puede elegir crear particiones del tipo *disco flexible* o *disco duro*. No está admitido el tipo de partición CD en la creación de particiones vacías.

NOTA: Debe tener privilegios de acceso a los medios virtuales para crear particiones vacías.

Antes de crear una partición vacía, asegúrese de lo siguiente:

- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

Para crear una partición vFlash vacía:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema**→ **vFlash**, subficha→ **Crear partición vacía**. Aparece la página **Crear partición vacía**.
2. Introduzca la información que se indica en Tabla 11-2.
3. Haga clic en **Aplicar**. Se crea una nueva partición.

NOTA: Cuando está en curso la creación de una partición, no se muestra el progreso o estado

Aparece un mensaje de error si:

- La tarjeta está protegida contra escritura.
- El nombre de la etiqueta coincide con la etiqueta de una partición existente.
- Se escribe un valor no entero como tamaño de la partición, el valor excede el tamaño disponible de la tarjeta o el tamaño de la partición solicitado es mayor de 4 GB.
- Ya se está realizando una operación de inicialización en la tarjeta.

NOTA: La nueva partición no está formateada (RAW).

Tabla 11-2. Opciones de la página Creación de una partición vacía

Campo	Descripción
Índice	Seleccione un índice de partición. Sólo se muestran los índices no utilizados en la lista desplegable. En forma predeterminada, se selecciona el índice disponible más bajo. Puede cambiarlo a cualquier otro valor de índice de la lista desplegable. **NOTA:** Para la tarjeta SD estándar, sólo está disponible el índice 1.
Etiqueta	Introduzca una etiqueta exclusiva para la nueva partición. El nombre de la etiqueta puede contener hasta seis caracteres alfanuméricos. No incluya ningún espacio en el nombre de la etiqueta. Los caracteres se muestran en mayúsculas. **NOTA:** Para la tarjeta SD estándar, el nombre de etiqueta debe ser VFLASH. De lo contrario, aparece un mensaje de error.
Tipo de emulación	Seleccione el tipo de emulación para la partición en la lista desplegable. Las opciones disponibles son **Disco flexible** y **HDD** (Unidad de disco duro).
Tamaño	Escriba el tamaño de la partición en Megabytes (MB). El tamaño máximo de la partición es 4 GB, o menor o igual al espacio disponible en la tarjeta vFlash SD. **NOTA:** Para la tarjeta SD estándar, el tamaño de la partición puede alcanzar 256 MB.

Creación de una partición utilizando un archivo de imagen

Se puede crear una partición nueva en una tarjeta SD estándar o vFlash mediante un archivo de imagen (disponible en formato **.img** o **.iso**). Se puede crear una partición de tipo disco flexible, disco duro o CD. La partición creada es de sólo lectura.

NOTA: Para crear particiones debe tener privilegios de acceso a medios virtuales.

El tamaño de la partición recién creada es igual al tamaño del archivo de imagen. El tamaño del archivo de imagen debe ser:

- Menor o igual que el espacio disponible en la tarjeta.
- Menor o igual a 4 GB. El tamaño máximo de la partición es de 4 GB.

Utilizando la interfaz web, el tamaño de imagen que se puede cargar en la tarjeta vFlash SD está limitado a un máximo de 2 GB en exploradores de 32 bits y de 64 bits (Internet Explorer y FireFox).

Utilizando la interfaz de racadm y WSMAN, el tamaño de la imagen que se puede cargar en la tarjeta vFlash SD es de un máximo de 4 GB.

Para la tarjeta SD estándar, el tamaño de la imagen debe ser menor o igual a 256MB.

Antes de crear una partición para un archivo de imagen, asegúrese de lo siguiente:

- La tarjeta está inicializada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

NOTA: Al crear una partición desde un archivo de imagen, asegúrese de que el tipo de imagen y el tipo de emulación coincidan. iDRAC emula el dispositivo en base al tipo de imagen especificado. Podría haber problemas cuando la imagen cargada y el tipo de emulación no coinciden. Por ejemplo, si la partición se crea utilizando una imagen ISO y el tipo de emulación se especifica como disco duro, entonces el BIOS no podrá iniciarse a partir de esta imagen.

Para crear una partición vFlash utilizando un archivo de imagen:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash** subficha→ **Crear a partir de imagen**. Aparece la página **Crear partición a partir de un archivo de imagen**.
2. Introduzca la información que se indica en Tabla 11-3.

3 Haga clic en **Aplicar**. Se crea una partición nueva utilizando el archivo de imagen.

NOTA: Cuando está en curso la creación de una partición, no se muestra el progreso o estado

Aparece un mensaje de error si:

- La tarjeta está protegida contra escritura.
- El nombre de la etiqueta coincide con la etiqueta de una partición existente.
- El tamaño de la imagen es mayor de 4 GB o excede el espacio disponible en la tarjeta.
- El archivo de imagen no existe o la extensión del archivo de imagen no es **.img** ni **.iso**.
- Ya se está realizando una operación de inicialización en la tarjeta.

Tabla 11-3. Opciones de la página Creación de una partición desde un archivo de imagen

Campo	Descripción
Índice	Seleccione un índice de partición. Sólo se muestran los índices no utilizados en la lista desplegable. En forma predeterminada, se selecciona el índice disponible más bajo. Puede cambiarlo a cualquier otro valor de índice de la lista desplegable. **NOTA:** Para la tarjeta SD estándar, sólo está disponible el índice 1.
Etiqueta	Introduzca una etiqueta exclusiva para la nueva partición. Ésta puede contener hasta seis caracteres alfanuméricos. No incluya espacios en el nombre de la etiqueta. Los caracteres se muestran en mayúsculas. **NOTA:** Para la tarjeta SD estándar, el nombre de etiqueta debe ser VFLASH. De lo contrario, aparece un mensaje de error.
Tipo de emulación	Seleccione el tipo de emulación para la partición en la lista desplegable. Las opciones disponibles son **Disco flexible**, **HDD** y **CD-ROM**.

Tabla 11-3. Opciones de la página Creación de una partición desde un archivo de imagen *(continuación)*

Campo	Descripción
Ubicación de la imagen	Haga clic en **Examinar** y especifique la ubicación del archivo de imagen. Sólo se admiten los tipos de archivo **.img** o **.iso**.

Formateo de una partición

Se puede formatear una partición existente en la tarjeta vFlash SD con base en el tipo de sistema de archivos. Los tipos de sistemas de archivos admitidos son EXT2, EXT3, FAT16 y FAT32. La tarjeta SD estándar con funciones de vFlash limitadas admite sólo el formato FAT32.

Sólo se pueden formatear particiones de tipo Disco duro o Disco flexible. No se admite el formateo de particiones de CD. No se pueden formatear las particiones de sólo lectura.

NOTA: Debe tener privilegios de acceso a los medios virtuales para formatear particiones.

Antes de formatear la partición, asegúrese de lo siguiente:

- La tarjeta está activada.
- La partición no está conectada.
- La tarjeta no está protegida contra escritura.
- No se está realizando una operación de inicialización en la tarjeta.

Para formatear la partición vFlash:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Formatear**. Aparece la página **Formatear**.
2. Introduzca la información que se indica en Tabla 11-4.
3. Haga clic en **Aplicar**. Aparece un mensaje de advertencia que indica que todos los datos de la partición se borrarán. Haga clic en **OK** (Aceptar). La partición seleccionada se formatea con el tipo de sistema de archivos especificado.

   Aparece un mensaje de error si:

   - La tarjeta está protegida contra escritura.
   - Ya se está realizando una operación de inicialización en la tarjeta.

Tabla 11-4. Opciones de la página Formatear partición

Campo	Descripción
Etiqueta	Seleccione la etiqueta de la partición que desea formatear. Se selecciona la primera partición disponible de manera predeterminada. Todas las particiones existentes de tipo disco flexible o disco duro están disponibles en la lista desplegable. Las particiones que no están conectadas o que son de sólo lectura no están disponibles en la lista desplegable.
Tipo de formato	Seleccione el tipo de sistema de archivos conforme al que desea formatear la partición. Las opciones disponibles son EXT2, EXT3, FAT16 y FAT32. Para la tarjeta SD estándar, sólo está disponible el tipo FAT32.

Visualización de las particiones disponibles

Compruebe que la tarjeta SD estándar o vFlash está activada para ver la lista de particiones disponibles.

Para ver las particiones disponibles en la tarjeta:

1. En la interfaz web del iDRAC6, seleccione **Sistema→ vFlash** subficha→ **Administrar**. La página **Administrar particiones** indica las particiones disponibles.
2. Para cada partición, se puede ver la información incluida en la Tabla 11-5.

Tabla 11-5. Visualización de las particiones disponibles

Campo	Descripción
Índice	Las particiones tienen un número de índice de 1 a 16. El índice de la partición es exclusivo para una partición específica. Se especifica cuando se crea una partición.
Etiqueta	Identifica la partición. Se especifica cuando se crea una partición.
Tamaño	Tamaño de la partición en Megabytes (MB).

Tabla 11-5. Visualización de las particiones disponibles

Campo	Descripción
Sólo lectura	Estado del acceso de lectura y escritura de la partición. • Marcado = Partición de sólo lectura. • No marcado = Partición de lectura y escritura. **NOTA:** Para la tarjeta SD estándar, la partición es de lectura y escritura, y esta columna no aparece.
Conectado	Indica si la partición es visible para el sistema operativo como un dispositivo USB. Para conectar o desconectar las particiones, consulte la sección "Cómo conectar y desconectar una partición" en la página 266.
Escriba	Muestra si el tipo de la partición es disco flexible, disco duro o CD.

Modificación de una partición

Asegúrese de que la tarjeta esté activada para modificar la partición.

NOTA: Para modificar una partición vFlash debe tener privilegios de acceso a medios virtuales.

Se puede cambiar una partición de sólo lectura a lectura y escritura, y viceversa. Para hacer esto:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Sólo lectura**, seleccione la casilla de marcación de las particiones que desea cambiar a sólo lectura o desmarque la casilla de las particiones que desea cambiar a lectura-escritura.

NOTA: Si la partición es de tipo CD, el estado es sólo lectura y la casilla de marcación está seleccionada. El estado no se puede cambiar a lectura y escritura. Si la partición está conectada, la casilla de marcación aparece en gris. Para la tarjeta SD estándar, la partición es de lectura-escritura y la columna **Sólo lectura** no aparece.

3. Haga clic en **Aplicar**. Las particiones se cambian a sólo lectura o lectura y escritura con base en las selecciones.

Cómo conectar y desconectar una partición

Se puede adjuntar una o más particiones como dispositivos de almacenamiento masivo USB virtuales de manera que sean visibles para el sistema operativo y el BIOS como dispositivos de almacenamiento masivo. Cuando se conectan varias particiones simultáneamente, se presentan en orden ascendente al sistema operativo host conforme al índice. La asignación de la letra de unidad correspondiente es controlada por el sistema operativo.

Si se desconecta una partición, ya no se ve como un dispositivo de almacenamiento masivo USB virtual en el sistema operativo host y se elimina del menú de orden de inicio del BIOS.

Si se está conectando o desconectando una partición, el bus USB del sistema se restablece. Esto puede afectar las aplicaciones (como el sistema operativo= que están utilizando vFlash y se desconecta cualquier sesión de medios virtuales del iDRAC.

NOTA: Debe tener privilegios de acceso a los medios virtuales para conectar o desconectar una partición.

Antes de conectar o desconectar una partición, asegúrese de lo siguiente:

- La tarjeta está activada.
- No se está realizando una operación de inicialización en la tarjeta.

Para conectar o desconectar particiones:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Conectada**, seleccione la casilla de marcación para las particiones que desea conectar, o quite la marca de la casilla de marcación para las particiones que desea desconectar.

NOTA: Las particiones desconectadas no aparecen en la secuencia de inicio.

3. Haga clic en **Aplicar**. Las particiones se conectan o desconectan conforme a las selecciones.

Comportamiento del sistema operativo para las particiones adjuntas

Cuando las particiones están conectadas y el sistema operativo host es Windows, el sistema operativo controla las letras de unidad que se asignan a las particiones conectadas.

Si una partición es de sólo lectura, será de sólo lectura como se ve en el sistema operativo host.

Si el sistema operativo host no admite el sistema de archivos de una partición conectada, no se puede leer ni modificar el contenido de la partición desde el sistema operativo host. Por ejemplo, una partición de tipo EXT2 no se puede leer desde el sistema operativo Windows.

Cuando se cambia el nombre de la etiqueta de una partición conectada desde el sistema operativo host, esto no afecta el nombre de la etiqueta almacenado en el iDRAC para esa partición.

Eliminación de las particiones existentes

NOTA: Las particiones existentes se pueden eliminar en la tarjeta SD estándar o vFlash.

Antes de eliminar las particiones existentes, compruebe lo siguiente:

- La tarjeta no está protegida contra escritura.
- La partición no está conectada.
- No se está realizando una operación de inicialización en la tarjeta.

NOTA: Para modificar una partición debe tener privilegios de acceso a medios virtuales.

Para eliminar una partición existente:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Administrar**. Aparece la página **Administrar particiones**.
2. En la columna **Eliminar**, haga clic en el icono Eliminar para las particiones que desee eliminar y luego haga clic en **Aplicar**. Las particiones se eliminan.

Descarga del contenido de una partición

El contenido de una partición vFlash se puede descargar en una ubicación local o remota como un archivo de imagen en formato **.img** o **.iso**. Una ubicación local es en el sistema de administración desde el que se opera la interfaz web del iDRAC6. Ubicación remota es un sistema administrado.

NOTA: Debe tener privilegios de acceso a los medios virtuales para descargar particiones.

Antes de descargar el contenido a una ubicación local o remota, asegúrese de lo siguiente:

- La tarjeta está activada.
- No se está realizando una operación de inicialización en la tarjeta.
- En el caso de una partición de lectura y escritura, no debe estar conectada.

Para descargar el contenido de la partición vFlash a una ubicación en su sistema:

1. En la interfaz web del iDRAC6, seleccione la ficha **Sistema→ vFlash**, subficha→ **Descargar**. Aparece la página **Descargar partición**.

2 Desde el menú desplegable **Etiqueta**, seleccione una partición que desee descargar. Todas las particiones existentes se muestran en la lista, excepto las particiones que están conectadas. Se selecciona la primera partición de manera predeterminada.

3 Haga clic en **Descargar**.

4 Especifique la ubicación donde desea guardar el archivo.

Si sólo se especifica la ubicación de la carpeta, la etiqueta de la partición se usa como nombre del archivo, junto con la extensión **.iso** para las particiones de tipo CD y la extensión **.img** para las particiones de tipo disco flexible o disco duro.

5 Haga clic en **Save** (Guardar). El contenido de la partición seleccionada se descarga en la ubicación especificada.

Inicio de una partición

Se puede establecer una partición vFlash conectada como el dispositivo de inicio para la siguiente operación de inicio. La partición vFlash debe contener una imagen de inicio (en formato **.img** o **.iso**) para establecerla como dispositivo de inicio. Asegúrese de que la tarjeta esté activada para establecer una partición como dispositivo de inicio y realizar la operación de inicio.

NOTA: Debe tener privilegios de acceso a los medios virtuales para establecer una partición como el dispositivo de inicio.

Puede realizar la operación de inicio para la tarjeta SD estándar o vFlash. Para ver los pasos, consulte la sección "Primer dispositivo de inicio" en la página 49.

NOTA: Si el BIOS del sistema no admite vFlash como el primer dispositivo de inicio, es posible que las particiones vFlash conectadas no se encuentren en el menú desplegable **Primer dispositivo de inicio**. Por lo tanto, asegúrese de actualizar el BIOS con la versión más reciente que admita el establecimiento de la partición vFlash como el primer dispositivo de inicio. Si el BIOS es de la versión más reciente, al reiniciar el servidor el BIOS informa al iDRAC que admite vFlash como primer dispositivo de inicio y el iDRAC presenta la partición vFlash en el menú desplegable **Primer dispositivo de inicio**.

Administración de particiones vFlash mediante racadm

Se puede utilizar el subcomando `vFlashPartition` para crear, eliminar, enumerar o ver el estado de las particiones en una tarjeta SD estándar o vFlash ya inicializada. El formato es:

```
racadm vflashpartition <create | delete | status |
list> <options>
```

NOTA: Debe tener privilegios de acceso a los medios virtuales para llevar a cabo la administración de las particiones vFlash.

Opciones válidas:

-i <index>	Índice de la partición para la que se aplica este comando. <index> debe ser un número entero entre 1 y 16. **NOTA:** para la tarjeta SD estándar, el valor del índice se limita a 1 porque sólo se admite una partición de 256 MB.

Opciones válidas únicamente para la acción crear:

-o <label>	La etiqueta que se muestra cuando la partición se monta en un sistema operativo. <label> debe ser una cadena de hasta seis caracteres alfanuméricos y no debe contener espacios.
-e <type>	Tipo de emulación para la partición. <type> debe ser floppy, cd-rom o unidad de disco duro.

-t <type> Creación de un participación de tipo <tipo>. <type> debe ser:

- Vacío: crear una partición vacía.
  - -s <size>: tamaño de la partición en MB.
  - -f <type>: tipo de formato para la partición con base en el tipo de sistema de archivos. Las opciones válidas son RAW, FAT16, FAT32, EXT2 ó EXT3.
- imagen: crear una partición utilizando un archivo de imagen. Las siguientes opciones son válidas con el tipo de imagen:
  - -l <path>: especifica la ruta de acceso remota relativa al iDRAC. La ruta de acceso puede ser en una unidad montada o compartida.
    Ruta de acceso de SMB: //<ip or domain>/<share_name>/<path_to_image>
    Ruta de acceso de NFS: <ipaddress>:/<path_to_image>
  - -u <user>: nombre de usuario para acceder a la imagen remota.

-p <password>: contraseña para acceder a la imagen remota.

Opciones válidas únicamente para la acción estado:

-i Muestra el estado del índice de la partición.

Creación de una partición

- Para crear una partición vacía de 20 MB:

  ```
  racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20
  ```

- Para crear una partición utilizando un archivo de imagen de un sistema remoto:

  ```
  racadm vflashpartition create –i 1 –o drive1 –e HDD –t image –l //mi_servidor/sharedfolder/foo.iso –u root –p mi_contraseña
  ```

NOTA: La creación de una partición utilizando un archivo de imagen no se admite en racadm local.

Eliminación de una partición

- Para eliminar una partición:

  ```
  racadm vflashpartition delete -i 1
  ```

- Para eliminar todas las particiones, reinicialice la tarjeta vFlash SD. Para obtener más información, ver "Inicialización de la tarjeta SD estándar o vFlash" en la página 258.

Cómo obtener el estado de una partición

- Para obtener el estado de una operación en la partición 1:

  ```
  racadm vflashpartition status -i 1
  ```

- Para obtener el estado de todas las particiones existentes:

  ```
  racadm vflashpartition status -a
  ```

Visualización de la información de las particiones

Para ver una lista de todas las particiones existentes y sus propiedades:

```
racadm vflashpartition list
```

Inicio de una partición

- Para enumerar los dispositivos disponibles en la lista de inicio:

  ```
  racadm  getconfig -g cfgServerInfo -o
  cfgServerFirstBootDevice
  ```

  Si se trata de una tarjeta vFlash SD, los nombres de etiqueta de las particiones adjuntas aparecen en la lista de inicio. Si es una tarjeta SD estándar y la partición está conectada, aparece VFLASH en la lista de inicio.

- Para establecer una partición vFlash como dispositivo de inicio:

  ```
  racadm  config -g cfgServerInfo -o
  cfgServerFirstBootDevice "<vFlash partition name>"
  ```

  donde: <vFlash partition name> es el nombre de etiqueta de la tarjeta vFlash SD o VFLASH es el nombre de la tarjeta SD estándar.

NOTA: Cuando se ejecuta este comando, la etiqueta de partición vFlash automáticamente se configura en iniciar una vez, es decir: **cfgserverBootOnce** se configura en 1. Iniciar una vez inicia el dispositivo desde la partición sólo una vez y no persiste en mantenerlo primero en el orden de inicio.

Conexión o desconexión de una partición

- Para conectar una partición:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 1
  ```

- Para desconectar una partición:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 0
  ```

Modificación de una partición

- Para cambiar una partición de sólo lectura a lectura y escritura:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 1
  ```

- Para cambiar una partición de lectura y escritura a sólo lectura:

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 0
  ```

Para obtener más información acerca de los subcomandos RACADM y las definiciones de grupos y objetos de bases de datos de propiedades del iDRAC6, consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Preguntas frecuentes

¿Cuándo se bloquea la tarjeta SD estándar o vFlash?

El iDRAC bloquea los medios flash virtuales cuando la operación que está realizando requiere de acceso exclusivo a los medios. Por ejemplo, durante una operación de inicialización.

A veces, si intenta borrar la misma partición en el RACADM local, después de haber creado una partición, aparecerá un mensaje de error. ¿Por qué?

Es posible que ocurra cuando se encuentra en curso una operación de creación de partición. Sin embargo, la partición se borrará tras un tiempo y aparecerá un mensaje indicando que la partición ha sido borrada. Si no es así, espere a que finalice la operación de creación de partición y borre la partición a continuación.

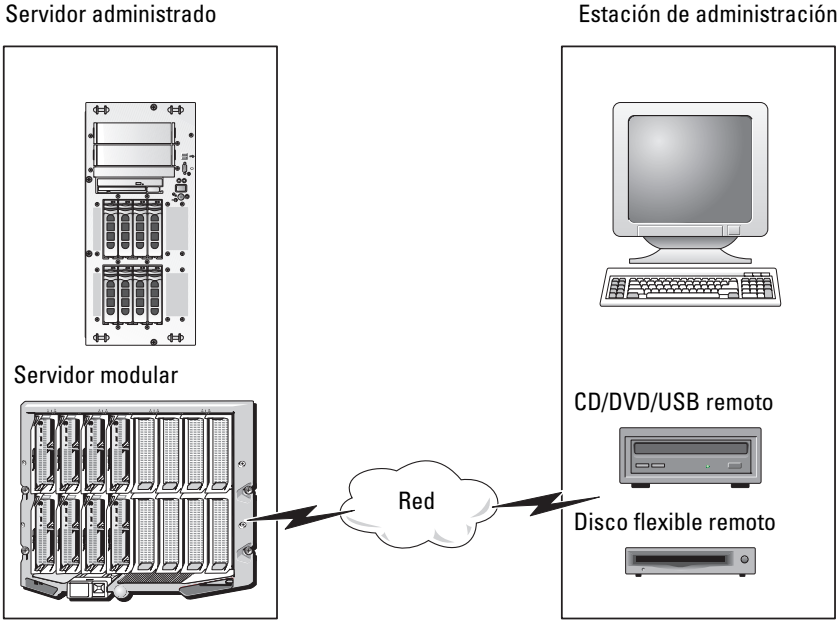
12

Configuración y uso de medios virtuales

Descripción general

La función Medios virtuales, a la que se puede acceder mediante el visor de la consola virtual, proporciona al servidor administrado acceso a medios conectados a un sistema remoto en la red. La Ilustración 12-1 muestra la arquitectura general de los medios virtuales.

Ilustración 12-1. Arquitectura general de medios virtuales



Por medio de los medios virtuales, los administradores pueden iniciar los servidores administrados, instalar aplicaciones, actualizar controladores o incluso instalar nuevos sistemas operativos de manera remota desde unidades CD/DVD y discos virtuales.

NOTA: Los medios virtuales requieren un ancho de banda de red mínima disponible de 128 Kbps.

Los medios virtuales definen dos dispositivos para el sistema operativo y el BIOS del servidor administrado: Un dispositivo de disco flexible y otro de disco óptico.

La estación de administración proporciona los medios físicos o el archivo de imagen a través de la red. Cuando los medios virtuales se conectan, todas las solicitudes de acceso a la unidad virtual de CD o de disco flexible provenientes del servidor administrado son dirigidas a la estación de administración por la red. Conectar los medios virtuales se asimila a insertar un soporte en un dispositivo físico del sistema administrado. Cuando los medios virtuales están en estado de conexión, los dispositivos virtuales en el sistema administrado aparecen como dos unidades sin los medios instalados.

La Tabla 12-1 enumera las conexiones compatibles de unidades ópticas virtuales y de discos flexibles virtuales.

NOTA: Si cambia los medios virtuales mientras están conectados podría detenerse la secuencia de inicio del sistema.

Tabla 12-1. Conexiones de unidad admitidas

Conexiones admitidas de unidad de disco virtual	Conexiones admitidas de unidad de disco óptico virtual
Unidad de disco flexible heredada de 1,44 con disco flexible de 1,44	Unidad combinada de CD-ROM, DVD, CD-RW, con medios CD-ROM
Unidad de disco flexible USB con un disco flexible de 1,44	Archivo de imagen de CD-ROM/DVD en el formato ISO9660
Imagen de disco flexible de 1,44	Unidad de CD-ROM USB con medios CD-ROM
Disco USB extraíble (tamaño mínimo de 128 MB)	

Estación de administración basada en Windows

Para ejecutar la función de medios virtuales en la estación de administración que está ejecutando el sistema operativo Windows, instale una versión compatible de Internet Explorer con el complemento de control ActiveX. Establezca la seguridad del explorador en el nivel **medio** o en un nivel inferior para permitir que Internet Explorer descargue e instale los controles ActiveX firmados.

Dependiendo de la versión de Internet Explorer, es posible que se le solicite una configuración de seguridad personalizada para ActiveX:

1. Inicie Internet Explorer.
2. Haga clic en **Herramientas→ Opciones de Internet** y después haga clic sobre la ficha **Seguridad**.
3. En **Seleccionar una zona de contenido web para especificar su configuración de seguridad**, haga clic para seleccionar la zona deseada.
4. En **Nivel de seguridad para esta zona,** haga clic en **Nivel personalizado**.

   Aparece la ventana **Configuración de seguridad**.
5. En **Controles y complementos para ActiveX**, asegúrese de que las siguientes opciones estén fijadas en **Permitir**:
   - Permitir Scriptlets
   - Preguntar automáticamente si se debe usar un control ActiveX
   - Descargar los controles firmados para ActiveX
   - Descargar los controles no firmados para ActiveX
6. Haga clic sobre **Aceptar** para guardar cualquier cambio y cierre la ventana de **Configuración de seguridad**.
7. Haga clic en **Aceptar** para cerrar la ventana **Opciones de Internet**.
8. Reinicie Internet Explorer.

Se deben tener derechos de administrador para instalar ActiveX. Antes de instalar el control ActiveX, es posible que Internet Explorer muestre una advertencia de seguridad. Para completar el procedimiento de instalación del control ActiveX, acepte el control ActiveX cuando Internet Explorer muestre la advertencia de seguridad.

Estación de administración basada en Linux

Para ejecutar el componente de medios virtuales en una estación de administración que está ejecutando el sistema operativo Linux, instale una versión compatible de Firefox.

Se requiere Java Runtime Environment (JRE) para ejecutar el complemento de consola virtual. Puede descargar JRE desde el sitio **java.sun.com**.

Configuración de los medios virtuales

1. Inicie sesión en la interfaz web del iDRAC6.
2. Haga clic en **Sistema→ Consola/Medios virtuales→ Configuración**.
3. En la sección Medios virtuales, seleccione los valores para la configuración. Ver Tabla 12-2 para obtener información acerca de los valores de configuración de los medios virtuales.
4. Haga clic en **Aplicar** para guardar la configuración.

   Aparecerá un cuadro de diálogo de alerta con el siguiente mensaje:
   `Está a punto de cambiar la configuración del dispositivo. Se cerrarán todas las sesiones de redirección existentes. Do you want to continue?`
5. Haga clic en **Aceptar** para continuar.

   Aparecerá un cuadro de diálogo de alerta con el siguiente mensaje:
   `La configuración de los medios virtuales se definió correctamente.`

Tabla 12-2. Valores de configuración de los medios virtuales

Atributo	Valor
Conectar medios virtuales	**Conectar**: Conecta inmediatamente los medios virtuales al servidor.
	Desconectar: Desconecta inmediatamente los medios virtuales del servidor.
	Conectar automáticamente: Conecta los medios virtuales al servidor únicamente cuando se inicia una sesión de medios virtuales.

Tabla 12-2. Valores de configuración de los medios virtuales *(continuación)*

Atributo	Valor
Número máximo de sesiones	Muestra el número máximo de sesiones de Medios virtuales permitidas. Este valor siempre es 1. **NOTA:** Sólo se permite una única sesión de medios virtuales. Sin embargo, en ella se pueden conectar múltiples dispositivos. Vea la "Ejecución de los medios virtuales" en la página 280.
Sesiones activas	Muestra la cantidad de sesiones de medios virtuales actualmente activas.
Cifrado activado para medios virtuales	Activa (seleccionada) o desactiva (deseleccionada) el cifrado de las conexiones de Medios virtuales.
Emulación de disco flexible	Indica si los **medios virtuales** aparecen como unidad de disco flexible o como memoria USB en el servidor. Si se selecciona **Emulación de disco flexible**, el dispositivo de medios virtuales aparecerá como dispositivo de disco flexible en el servidor. Cuando se deselecciona, aparece como unidad de memoria USB. **NOTA:** En determinados entornos de Windows Vista y Red Hat Enterprise Linux, existe la posibilidad de que no se pueda virtualizar una unidad USB con la opción **Emulación de disco flexible** activada.
Activar el inicio único	Activa (seleccionada) o desactiva (deseleccionada) la opción de inicio único, que cierra automáticamente la sesión de los Medios virtuales después de que el servidor se haya iniciado una vez. Utilice este atributo para iniciar el sistema desde los medios virtuales. En el próximo inicio, el sistema se iniciará desde el siguiente dispositivo en el orden de inicio. Esta opción es útil para implementaciones automáticas.

Ejecución de los medios virtuales

PRECAUCIÓN: No ejecute un comando racreset cuando esté ejecutando una sesión de medios virtuales. De lo contrario, se pueden presentar resultados inesperados, incluida la pérdida de datos.

NOTA: La aplicación de la ventana del visor de consola virtual debe permanecer activa mientras accede a los medios virtuales.

1. Abra un explorador web compatible en la estación de administración.
2. Inicie sesión en la interfaz web del iDRAC6.
3. Haga clic en la ficha **Consola/Medios virtuales**.

   Aparece la página **Consola virtual y Medios virtuales**.

   Para cambiar los valores de cualquiera de los atributos mostrados, ver "Configuración de los medios virtuales" en la página 278.

   NOTA: Es posible que aparezca **Archivo de imagen de disco flexible** bajo **Unidad de disco flexible** (si se aplica), pues este dispositivo se puede virtualizar como un disco virtual. Puede seleccionar una unidad óptica y un disco flexible al mismo tiempo, o una sola unidad.

   NOTA: Las letras de unidad de los dispositivos virtuales del servidor administrado no coinciden con las letras de las unidades físicas de la estación de administración.

   NOTA: Es posible que los medios virtuales no funcionen correctamente en los clientes con sistema operativo Windows configurados con seguridad mejorada en Internet Explorer. Para resolver este problema, consulte la documentación del sistema operativo de Microsoft o comuníquese con el administrador.
4. Haga clic en **Iniciar consola virtual**.

   NOTA: En Linux, el archivo **jviewer.jnlp** se descarga en el escritorio y un cuadro de diálogo pregunta qué desea hacer con el archivo. Elija la opción de **Abrir con el programa** y después seleccione la aplicación **javaws**, que se encuentra en el subdirectorio **bin** del directorio de instalación de JRE.

   La aplicación **iDRACView** se ejecuta en una ventana por separado.
5. Seleccione **Medios→ Asistente de medios virtuales**.

   Aparecerá el asistente **Redirección de medios**.

6 Consulte la sección **Estado** en la parte inferior de la ventana **Redirección de medios**. Si hay algún medio conectado, podrá desconectarlo antes de conectar otro medio. Para desconectar medios, haga clic en el botón **Desconectar** situado junto al medio en la ventana **Estado**.

7 Seleccione el botón de radio que está junto a los tipos de medios que desea conectar.

8 Puede seleccionar el botón de radio **Imagen de disco flexible** y uno de los botones de radio de la sección **Unidad de CD/DVD**.

NOTA: Si el medio de CD/DVD de la estación de administración está siendo usado por una tarjeta del iDRAC6, el mismo medio puede redirigirse y ponerse a la disposición de otra tarjeta del iDRAC6. En otras palabras, el iDRAC6 admite la redirección de un mismo medio (sólo lectura) hacia dos tarjetas del iDRAC6 diferentes. Sin embargo, con un medio USB no podrá conectarse a dos tarjetas del iDRAC6. El iDRAC6 muestra un mensaje de advertencia que indica lo mismo.

Para conectar una imagen de disco flexible o una imagen ISO, introduzca la ruta de acceso a la ubicación de la imagen en su equipo local o haga clic en el botón **Examinar** para desplazarse hasta la ubicación de la imagen.

NOTA: No podrá montar imágenes ISO remotas si utiliza el complemento Java de medios virtuales. Por ejemplo, los clientes Linux no le permitirán montar las imágenes debido a que usan el complemento Java. Para evitar este problema, copie la imagen ISO en el sistema local de modo que el archivo de imagen esté disponible de forma local. El complemento Java de medios virtuales no le permite especificar el nombre del recurso compartido mediante el formato **\\computer\share**.

9 Haga clic en el botón **Conectar** que se encuentra junto a cada tipo de medio seleccionado.

Los medios están conectados y la ventana de **estado** se actualiza.

10 Haga clic en **Cerrar**.

NOTA: Siempre que se inicia una sesión de medios virtuales o se conecta una unidad vFlash, aparece una unidad adicional denominada "LCDRIVE" en el sistema operativo del host y en el BIOS. La unidad adicional desaparece cuando la unidad vFlash o la sesión de medios virtuales se desconectan.

Desconexión de los medios virtuales

1 Seleccione **Medios→ Asistente de medios virtuales.**

Aparecerá el **Asistente de redirección de medios**.

2 Haga clic en **Desconectar** junto al medio que desea desconectar.

Los medios se desconectan y se actualiza la ventana de **estado**.

3 Haga clic en **Close** (Cerrar).

NOTA: Cuando inicia **iDRACview** y luego se desconecta de la interfaz gráfica del usuario de web, **iDRACView** no finaliza y permanece activo.

Inicio desde los medios virtuales

El BIOS del sistema le permite iniciar desde unidades ópticas virtuales o desde unidades de disco virtuales. Durante la POST, ingrese a la ventana de configuración del BIOS y verifique que las unidades virtuales estén activadas y que aparezcan en el orden correcto.

Para cambiar configuración del BIOS, realice los pasos a continuación:

1 Inicie el servidor administrado.

2 Presione <F2> para ingresar a la ventana de configuración del BIOS.

3 Desplácese a la secuencia de inicio y presione <Intro>.

En la ventana emergente, aparece una lista de las unidades ópticas virtuales y de discos virtuales con los dispositivos estándar de inicio.

4 Asegúrese de que la unidad virtual esté activada y que aparezca como el primer dispositivo con un medio de inicio. Si es necesario, siga las instrucciones que aparecen en la pantalla para modificar el orden de inicio.

5 Guarde los cambios y salga.

El servidor administrado se reinicia.

El servidor administrado intenta iniciarse a partir de un dispositivo de inicio con base en el orden de inicio. Si el dispositivo virtual está conectado y un medio de inicio está presente, el sistema se inicia a partir del dispositivo virtual. De lo contrario, el sistema ignora el dispositivo; como ocurriría con un dispositivo físico que no tiene medios de inicio.

Instalación de sistemas operativos mediante medios virtuales

Esta sección describe un método manual e interactivo para instalar el sistema operativo en la estación de administración que puede tardar varias horas en completarse. El procedimiento de instalación del sistema operativo con secuencias de comandos por medio de los Medios virtuales puede tardar menos de 15 minutos en terminar. Ver "Implementación del sistema operativo" en la página 353 para obtener más información.

1. Verifique lo siguiente:
   - El DVD/CD de instalación del sistema operativo está insertado en la unidad de DVD/CD de la estación de administración.
   - La unidad de DVD/CD local está seleccionada.
   - Está conectado a las unidades virtuales.
2. Siga los pasos para iniciar desde los medios virtuales que aparecen en la sección "Inicio desde los medios virtuales" en la página 282 para asegurarse de que el BIOS esté configurado para que inicie desde la unidad de DVD/CD desde donde se realiza la instalación.
3. Siga las instrucciones que aparecen en la pantalla para completar la instalación.

Uso de medios virtuales cuando el sistema operativo del servidor está en ejecución

Sistemas con Windows

En los sistemas Windows, las unidades de medios virtuales se montan automáticamente si están conectadas y configuradas con una letra de unidad.

El uso de las unidades virtuales desde Windows es similar al uso de las unidades físicas. Cuando se conecta a los medios por medio del asistente de medios virtuales, los medios estarán disponibles en el sistema cuando se haga clic en la unidad y se examine el contenido de la misma.

Sistemas basados en Linux

En función de la configuración del software del sistema, es posible que las unidades de medios virtuales no se monten automáticamente. Si las unidades no se montan automáticamente, monte manualmente las unidades con el comando **mount** de Linux.

Preguntas frecuentes

La Tabla 12-3 contiene las preguntas y respuestas frecuentes.

Tabla 12-3. Uso de los medios virtuales: preguntas frecuentes

Pregunta	Respuesta
Algunas veces noto que mi conexión de cliente de medios virtuales se cierra. ¿Por qué?	Cuando se agota el tiempo de espera de la red, el firmware de iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Si los valores de configuración de los medios virtuales se cambian en la interfaz web del iDRAC6 o con los comandos de RACADM local, se desconectarán todos los medios conectados al momento de aplicar el cambio de configuración. Para restablecer la conexión con la unidad virtual, use el asistente de medios virtuales.
¿Qué sistemas operativos son admitidos por el iDRAC6?	Consulte "Sistemas operativos compatibles" en la página 27 para ver una lista de los sistemas operativos compatibles.
¿Qué exploradores web son admitidos por el iDRAC6?	Consulte "Exploradores web admitidos" en la página 27 para ver una lista de los exploradores de web admitidos.

Tabla 12-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Por qué a veces se pierde mi conexión de cliente?	• Algunas veces, puede perder la conexión de cliente si la red es lenta o si cambia el CD en la unidad de CD del sistema cliente. Por ejemplo, si cambia el CD en la unidad de CD del sistema cliente, el nuevo CD podría tener una función de inicio automático. Si éste es el caso, el firmware puede agotar el tiempo de espera y se puede perder la conexión si el sistema cliente tarda demasiado en estar listo para leer el CD. Si la conexión se cierra, vuelva a conectarla desde la interfaz gráfica de usuario y continúe con la operación anterior. • Cuando se agota el tiempo de espera de la red, el firmware de iDRAC6 abandona la conexión y desconecta el vínculo entre el servidor y la unidad virtual. Asimismo, alguien puede haber cambiado los valores de configuración de los medios virtuales en la interfaz web o mediante comandos de RADACM. Para restablecer la conexión con el disco virtual, use la función de Medios virtuales.
La instalación del sistema operativo Windows parece tardar demasiado. ¿Por qué?	Si instala el sistema operativo Windows y la conexión de red es lenta, es posible que la instalación requiera más tiempo para acceder a la interfaz web del iDRAC6 debido a la latencia de la red. Aunque la ventana de instalación no indique el progreso de la instalación, el procedimiento de instalación está teniendo lugar.
Veo el contenido de una unidad de disco flexible o memoria USB. Si trato de establecer una conexión de medios virtuales con la misma unidad, recibo un mensaje de falla de conexión y se me pide que vuelva a intentarlo. ¿Por qué?	No se permite el acceso simultáneo a las unidades de disco virtual. Cierre la aplicación utilizada para ver el contenido de la unidad antes de que intente hacer virtual la unidad.

Tabla 12-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
¿Cómo configuro mi dispositivo virtual como dispositivo de inicio?	En el servidor administrado, acceda a la configuración del BIOS y vaya al menú de inicio. Localice el CD virtual, el disco virtual o la memoria vFlash y cambie el orden de los dispositivos de inicio según corresponda. Por ejemplo, para iniciar a partir de una unidad de CD, configure ésta como la primera unidad en el orden de inicio.
¿Desde qué tipos de medios puedo iniciar el sistema?	El iDRAC6 permite iniciar a partir de los siguientes medios de inicio: • Medios de CDROM/DVD de datos • Imagen ISO 9660 • Imagen de disco flexible o disco flexible de 1,44 • Una memoria USB que el sistema operativo reconozca como disco extraíble (tamaño mínimo de 128 MB) • Una imagen de memoria USB
¿Cómo puedo hacer que mi memoria USB sea de inicio?	Busque en **support.dell.com** la utilidad Dell Boot Utility, un programa para Windows que se puede usar para que la memoria USB de Dell funcione como dispositivo de inicio. Puede iniciar también con un disco de arranque de Windows 98 y copiar los archivos de sistema del disco de arranque a la memoria USB. Por ejemplo, desde una ventana de petición de comando DOS, introduzca el comando siguiente: `sys a: x: /s` donde *x*: es la memoria USB que desea hacer de inicio.
¿Qué tipo de sistemas de archivos son admitidos por la unidad de disco virtual?	Su unidad de disco virtual admite sistemas de archivos FAT16 o FAT32.
Cuando ejecuté una actualización de firmware de manera remota por medio de la interfaz web del iDRAC6, mis unidades virtuales en el servidor se desmontaron. ¿Por qué?	Las actualizaciones de firmware hacen que el iDRAC6 se restablezca, que abandone la conexión remota y que desmonte las unidades virtuales. Las unidades volverán a aparecer cuando el restablecimiento del iDRAC6 termine.

Tabla 12-3. Uso de los medios virtuales: preguntas frecuentes *(continuación)*

Pregunta	Respuesta
No puedo encontrar mi dispositivo de disco virtual en un sistema que ejecuta el sistema operativo Red Hat Enterprise Linux o SUSE Linux. Mis medios virtuales están conectados y estoy conectado a mi disco flexible remoto. ¿Qué debo hacer?	Algunas versiones de Linux no montan automáticamente la unidad de disco virtual y la unidad de CD virtual de manera similar. Para montar el dispositivo de disco flexible virtual, localice el nodo de dispositivo que Linux asigna a la unidad de disco virtual. Realice los pasos a continuación para encontrar y montar correctamente la unidad de disco flexible virtual: **1** Abra un símbolo del sistema de Linux y ejecute el siguiente comando: `grep "Disco virtual" /var/log/messages` **2** Localice la última entrada de dicho mensaje y anote la hora. **3** En la línea de comandos de Linux, ejecute el siguiente comando: `grep "hh:mm:ss" /var/log/messages` donde: *`hh:mm:ss`* es la hora del mensaje que el comando grep informó en el paso 1. **4** En el paso 3, lea el resultado del comando grep y localice el nombre del dispositivo que se asigna al disco flexible virtual Dell. **5** Asegúrese de que está conectado a la unidad de disco flexible virtual. **6** En la línea de comandos de Linux, ejecute el siguiente comando: mount */dev/sdx* /mnt/floppy donde: *`/dev/sdx`* es el nombre del dispositivo que se encontró en el paso 4 `/mnt/floppy` es el punto de montaje.

13

Uso de la interfaz de línea de comandos de RACADM

La interfaz de línea de comandos (CLI) de RACADM proporciona acceso a las funciones de administración del iDRAC6 en el servidor administrado. RACADM permite acceder a la mayoría de las funciones de la interfaz web del iDRAC6. RACADM se puede utilizar con secuencias de comandos para facilitar la configuración de varios servidores en lugar de utilizar la interfaz web, que es más útil para la administración interactiva.

Las siguientes interfaces están disponibles para RACADM:

- RACADM local
- RACADM remoto
- RACADM Telnet/SSH

Los comandos de RACADM local no utilizan las conexiones de red para acceder al iDRAC6 desde el servidor administrado. Esto significa que los comandos de RACADM local se pueden utilizar para configurar el sistema inicial de red del iDRAC6. RACADM remoto es una utilidad en el cliente que puede ejecutarse desde una estación de administración a través de la interfaz de red fuera de banda. RACADM SSH/Telnet se utiliza para hacer referencia al uso del comando de RACADM desde un símbolo del sistema SSH o Telnet.

En esta sección se proporciona la información siguiente:

- Comandos RACADM e interfaces admitidas de RACADM
- Uso de RACADM local desde el símbolo del sistema
- RACADM remoto
- RACADM SSH/Telnet
- Configuración del iDRAC6 por medio del comando **racadm**
- Uso del archivo de configuración de RACADM para configurar varios iDRAC6

PRECAUCIÓN: El firmware más reciente del iDRAC6 admite únicamente la versión más reciente de RACADM. Es posible que encuentre errores si utiliza una versión anterior de RACADM para consultar el iDRAC6 que tiene el firmware más reciente. Instale la versión de RACADM que se incluye con su DVD más reciente de Dell OpenManage.

Subcomandos de RACADM

Tabla 13-1 proporciona una descripción de cada uno de los subcomandos de RACADM que se pueden ejecutar en RACADM. Para obtener una lista detallada de los subcomandos RACADM incluida la sintaxis y las anotaciones válidas, consulte la *Guía de referencia de la línea de comandos RACADM para iDRAC y CMC* adisponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Tabla 13-1. Subcomandos de RACADM

Comando	Descripción
arp	Muestra el contenido de la tabla ARP. Los registros de la tabla ARP no se pueden agregar ni eliminar.
clearasrscreen	Borra la pantalla de último bloqueo (ASR).
closessn	Cierra una sesión de comunicación en el dispositivo.
coredump	Muestra el último volcado central del iDRAC6.
coredumpdelete	Borra el volcado central almacenado en el iDRAC6.
clrraclog	Borra el registro del iDRAC6. Después de borrarlo, sólo se hace una anotación para indicar el usuario que borró el registro y la hora en la que se borró.
clrsel	Borra las anotaciones del registro de sucesos del sistema iDRAC.
config	Configura el iDRAC6.
fwupdate	Actualiza el firmware del iDRAC6.
getconfig	Muestra las propiedades de configuración actuales del iDRAC6.
getniccfg	Muestra la configuración IP actual para la controladora.
getraclog	Muestra el registro del iDRAC6.
getractime	Muestra la hora del iDRAC6.
getsel	Muestra las anotaciones en el Registro de sucesos del sistema (SEL).
getssninfo[1]	Muestra información sobre las sesiones activas.
getsvctag	Muestra la etiqueta de servicio.

Tabla 13-1. Subcomandos de RACADM *(continuación)*

Comando	Descripción
getsysinfo	Muestra información sobre el iDRAC6 y el servidor administrado, incluida la configuración de IP, el modelo de hardware, las versiones de firmware y la información del sistema operativo.
gettracelog	Muestra el registro de rastreo del iDRAC6. Si se utiliza con `-i`, el comando muestra el número de anotaciones en el registro de rastreo del iDRAC6.
help	Enumera los subcomandos del iDRAC6.
help <subcomando>	Muestra la descripción de uso del subcomando especificado.
ifconfig	Muestra el contenido de la tabla de interfaz de red.
krbkeytabupload	Permite cargar un archivo keytab de Kerberos.
localconredirdisable	Desactiva la consola virtual local desde el sistema local.
netstat	Muestra la tabla de enrutamiento y las conexiones actuales.
ping	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se requiere una dirección IP de destino. Un paquete de eco de ICMP se envía a la dirección IP de destino en función del contenido de tabla de enrutamiento actual.
ping6	Verifica que se pueda acceder a la dirección IPv6 de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se requiere una dirección IPv6 de destino. Un paquete de eco de ICMP se envía a la dirección IPv6 de destino en función del contenido de la tabla de enrutamiento actual.
racdump	Muestra información general y del estado del iDRAC6.
racreset	Restablece la configuración del iDRAC6.
racresetcfg	Restablece la configuración predeterminada del iDRAC6.
remoteimage	Recurso de archivos compartidos remoto
serveraction	Realiza operaciones de administración de alimentación en el servidor administrado.
setniccfg	Establece la configuración IP de la controladora.

Tabla 13-1. Subcomandos de RACADM *(continuación)*

Comando	Descripción
sshpkauth	Permite cargar un máximo de 4 claves públicas SSH diferentes, eliminar claves existentes y ver las claves que ya se encuentran en el iDRAC6.
sslcertdownload	Descarga un certificado CA o un certificado de servidor desde iDRAC.
sslcertupload	Carga un certificado de CA o un certificado de servidor en el iDRAC6.
sslcertview	Muestra un certificado de CA o un certificado de servidor en el iDRAC6.
sslcsrgen	Genera y descarga la CSR de SSL.
testemail	Obliga al iDRAC6 a enviar un correo electrónico a través del NIC del iDRAC6.
testtrap	Obliga al iDRAC6 a enviar una alerta SNMP a través del NIC del iDRAC6.
traceroute	Rastrea la ruta de acceso a la red de enrutadores que toman los paquetes a medida que se reenvían desde el sistema hasta una dirección IPv4 de destino.
traceroute6	Rastrea la ruta de acceso a la red de enrutadores que los paquetes toman a medida que se reenvían desde el sistema hasta una dirección IPv6 de destino.
version	Muestra la información de versión del iDRAC6.
vflashsd	Inicializa u obtiene el estado de la tarjeta vFlash SD.
vflashpartition	Crea, elimina, enumera o visualiza el estado de las particiones en una tarjeta vFlash SD inicializada.
vmdisconnect	Cierra todas las conexiones de soportes virtuales del iDRAC6 desde los clientes remotos.
vmkey	Restablece la partición de vFlash al tamaño predeterminado de 256 MB y elimina todos los datos de la partición.

[1] No se incluye información de la sesión SOL en la respuesta al comando getssninfo.

Uso de comandos de RACADM local

Los comandos de RACADM se ejecutan de manera local (en el servidor administrado) desde el símbolo del sistema o petición de shell.

Inicie sesión en el servidor administrado, inicie un shell de comandos e introduzca comandos de RACADM local en alguno de los siguientes formatos:

- `racadm <subcommands> [parameters]`
- `racadm <getconfig|config> [-g <group>] [-o <object> <value>]`

Sin opciones, el comando de RACADM muestra la información general de uso. Para mostrar la lista de subcomandos de RACADM, introduzca:

```
racadm help
```

o

```
racadm getconfig -h
```

La lista de subcomandos incluye todos los comandos de RACADM compatibles con el iDRAC6.

Para obtener ayuda para un subcomando, introduzca:

`racadm help <subcomand>`

El comando muestra la sintaxis y las opciones de línea de comandos del subcomando.

NOTA: No se recomienda el uso de otros caracteres diferentes a los caracteres que no son alfanuméricos como, por ejemplo, $, %, <, >, | etc. en los argumentos de comando de RACADM. El uso de los mismos podría provocar un comportamiento inesperado.

Uso de la utilidad RACADM para configurar el iDRAC6

Esta sección describe cómo utilizar RACADM para realizar varias tareas de configuración del iDRAC6.

Visualización de la configuración actual del iDRAC6

El subcomando **getconfig** de RACADM obtiene los valores de configuración actuales del iDRAC6. Los valores de configuración se organizan en *grupos* que contienen uno o varios *objetos* y los objetos tienen *valores*.

Consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para obtener una descripción completa de los grupos y objetos.

Para mostrar una lista de todos los grupos de iDRAC6, introduzca este comando:

```
racadm getconfig -h
```

Para mostrar los objetos y valores de un grupo en particular, introduzca este comando:

```
racadm getconfig -g <group>
```

Por ejemplo, para mostrar una lista de todos los valores del objeto de grupo **cfgLanNetworking**, introduzca el comando siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Administración de usuarios del iDRAC6 con RACADM

NOTA: Tenga precaución cuando utilice el comando **racresetcfg**, pues se restablecerán *todos* los parámetros de configuración predeterminados originales. Todos los cambios anteriores se perderán.

NOTA: Si está configurando un iDRAC6 nuevo o si ha ejecutado el comando **racadm racresetcfg**, el único usuario actual es **root** con la contraseña **calvin**.

NOTA: Los usuarios se pueden activar o desactivar con el tiempo. Por consiguiente, un usuario puede tener un número de índice diferente en cada iDRAC6.

NOTA: Los usuarios y grupos creados para entornos de Active Directory deben cumplir con la convención de nombres de Active Directory.

Puede configurar hasta 15 usuarios en la base de datos de propiedades de iDRAC6. (El decimosexto usuario se reserva para el usuario de LAN de IPMI.) Antes de activar manualmente un usuario de iDRAC6, verifique si existe algún usuario actual.

Para verificar si existe un usuario, introduzca el comando siguiente en el símbolo del sistema:

```
racadm getconfig -u <username>
```

O bien:

introduzca el comando siguiente una vez para cada índice de 1 a 16:

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

NOTA: También puede introducir `racadm getconfig -f <filename>` y ver el archivo <*filename*> que se genera y que incluye a todos los usuarios, así como todos los demás parámetros de configuración del iDRAC6.

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

```
# cfgUserAdminIndex=nn

cfgUserAdminUserName=
```

Si el objeto **cfgUserAdminUserName** no tiene un valor, el número de índice que indica el objeto **cfgUserAdminIndex** está disponible para su uso. Si aparece un nombre después del signo =, significa que ese índice está asignado a ese nombre de usuario.

NOTA: Los usuarios y grupos creados para entornos de Active Directory deben cumplir con la convención de nombres de Active Directory.

Cómo agregar un usuario del iDRAC6

Para agregar un nuevo usuario al iDRAC6, realice los pasos a continuación:

1. Establezca el nombre de usuario.
2. Establezca la contraseña.
3. Establezca el privilegio de inicio de sesión en el iDRAC6 para el usuario.
4. Active el usuario.

Ejemplo

El ejemplo a continuación describe cómo agregar un nuevo usuario de nombre "Juan" con una contraseña "123456" y privilegios de inicio de sesión en el iDRAC6.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2 juan
```

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2 123456

racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -
i 2 1
```

Para verificar el usuario nuevo, utilice uno de los comandos siguientes:

```
racadm getconfig -u juan

racadm getconfig -g cfgUserAdmin -i 2
```

Activación de un usuario del iDRAC6 con permisos

Para otorgar permisos administrativos específicos (en base a funciones) a un usuario, configure la propiedad **cfgUserAdminPrivilege** con una máscara de bits creada a partir de los valores que se muestran en Tabla 13-2:

Tabla 13-2. Máscaras de bit para privilegios del usuario

Privilegio de usuario	Máscara de bits de privilegios
Iniciar sesión en el iDRAC6	0x00000001
Configurar el iDRAC6	0x00000002
Configurar usuarios	0x00000004
Borrar registros	0x00000008
Ejecutar comandos de control del servidor	0x00000010
Acceder a la consola virtual	0x00000020
Acceder a los medios virtuales	0x00000040
Probar alertas	0x00000080
Ejecutar comandos de depuración	0x00000100

Por ejemplo, para conceder al usuario privilegios para **Configurar el iDRAC6**, **Configurar usuarios**, **Borrar registros** y **Acceder a la consola virtual**, agregue los valores 0x00000002, 0x00000004, 0x00000008 y 0x00000010 para crear el mapa de bits 0x0000002E. Después introduzca el siguiente comando para establecer el privilegio:

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i 2 0x0000002E
```

Carga, visualización y eliminación de claves SSH usando RACADM

Cargar

El modo de carga permite cargar un archivo de clave o copiar el texto de la clave en la línea de comandos. No es posible cargar y copiar una clave al mismo tiempo.

En RACADM local:

```
racadm sshpkauth -i <2 a 16> -k <1 a 4> -f
<nombre_de_archivo>
```

En RACADM de Telnet/SSH:

```
racadm sshpkauth -i <2 a 16> -k <1 a 4> -t

<texto-de-la-clave>
```

Ejemplo:

Cargue una clave válida en el usuario 2 de iDRAC6 en el primer espacio de clave por medio de un archivo:

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

El archivo de clave de autentificación PK SSH se cargó correctamente en el RAC.

PRECAUCIÓN: La opción "archivo" no se admite en el RACADM de Telnet/SSH/Serie.

Ver

El modo de visualización le permite al usuario ver una clave que haya especificado o todas las claves.

```
racadm sshpkauth -i <2 a 16> -v -k <1 a 4>

racadm sshpkauth -i <2 a 16> -v -k all
```

Eliminar

El modo de eliminación le permite al usuario eliminar una clave que haya especificado o todas las claves.

```
racadm sshpkauth -i <2 a 16> -d -k <1 a 4>
racadm sshpkauth -i <2 a 16> -d -k all
```

PRECAUCIÓN: Este privilegio normalmente se reserva para usuarios que son miembros del grupo de usuarios Administrador de iDRAC. No obstante, se puede asignar este privilegio a los usuarios del grupo de usuarios "Personalizado". Un usuario con este privilegio puede modificar la configuración de cualquier usuario. Esto incluye la creación o eliminación de cualquier usuario, la administración de la clave SSH para usuarios, etc. Por estos motivos, asigne este privilegio con cuidado.

Consulte sshpkauth en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para obtener información sobre las opciones de los subcomandos.

Eliminación de un usuario del iDRAC6

Cuando se utiliza RACADM, el usuario del iDRAC no puede eliminarse. El usuario sólo puede ser desactivado mediante el objeto **cfgUserAdminEnable**. La sintaxis de los comandos es:

```
racadm config –g cfgUserAdmin –o cfgUserAdminEnable –I
<index>
```

Para obtener más información sobre la administración de los comandos "user admin", consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Pruebas de las alertas por correo electrónico

La función de alertas por correo electrónico del iDRAC6 permite al usuario recibir alertas por correo electrónico cuando se produce un suceso crítico en el servidor administrado. El siguiente ejemplo muestra cómo probar la función de alertas por correo electrónico para asegurarse de que el iDRAC6 pueda enviar correctamente alertas por correo electrónico a través de la red.

```
racadm testemail -i 2
```

(-i 2 corresponde a la entrada del índice n.º 2 en la tabla de alertas de correo electrónico)

NOTA: Asegúrese de que los valores de SMTP y de alerta por correo electrónico estén configurados antes de probar la función de alertas por correo electrónico. Ver "Configuración de alertas por correo electrónico" en la página 101 para obtener más información.

Prueba de la función de alertas de capturas SNMP del iDRAC6

La función de envío de alertas de capturas SNMP del iDRAC6 permite que las configuraciones de oyentes de capturas SNMP reciban capturas de los sucesos del sistema que se presentan en el servidor administrado.

El ejemplo a continuación muestra cómo un usuario puede probar la función de alertas de capturas SNMP.

```
racadm testtrap -i 2
```

(-i 2 corresponde a la entrada del índice n.º 2 en la tabla de alertas de correo electrónico)

NOTA: Antes de probar la función de alertas de capturas SNMP del iDRAC6, asegúrese de que los valores de captura y SNMP estén configurados correctamente. Consulte las descripciones de los subcomandos **testtrap** y **testemail** para configurar estos valores. Ver "Configuración de capturas de sucesos de plataforma (PET)" en la página 100 para obtener más información.

Configuración de las propiedades de red del iDRAC6

Para generar una lista de las propiedades de red disponibles, introduzca lo siguiente:

```
racadm getconfig -g cfgLanNetworking
```

Para utilizar DHCP para obtener una dirección IP, utilice el siguiente comando para escribir el objeto **cfgNicUseDhcp** y activar esta función:

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

Los comandos proporcionan la misma funcionalidad de configuración que la utilidad de configuración del iDRAC6 cuando se le pide que presione <Ctrl><E>. Para obtener más información acerca de la configuración de las propiedades de red con la utilidad de configuración del iDRAC6, ver "LAN del iDRAC6" en la página 365.

El siguiente es un ejemplo de cómo se pueden utilizar los comandos para configurar las propiedades de red LAN deseadas.

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

```
racadm config -g cfgLanNetworking -o cfgNicIpAddress
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask
255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1
192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2
192.168.0.6

racadm config -g cfgLanNetworking -o
cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName
RAC-EK00002

racadm config -g cfgLanNetworking -o
cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName
MI_DOMINIO
```

NOTA: Si **cfgNicEnable** se define en **0**, la LAN del iDRAC6 se desactivará aun cuando DHCP esté activado.

Configuración de IPMI en la LAN

1 Configure la IPMI en la LAN con el comando siguiente:

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

NOTA: Este valor determina los comandos de IPMI que se pueden ejecutar desde la interfaz IPMI en la LAN. Para obtener más información, consulte las especificaciones de IPMI 2.0.

a Actualice los privilegios de canal de IPMI con el comando siguiente:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit <nivel>
```

donde `<nivel>` es uno de los siguientes valores:

- `2` (**Usuario**)
- `3` (**Operador**)
- `4` (**Administrador**)

Por ejemplo, para establecer el privilegio de canal de LAN de IPMI en 2 (usuario), introduzca el comando siguiente:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit 2
```

b De ser necesario, defina la clave de cifrado del canal de la LAN de IPMI con un comando como el siguiente:

NOTA: La IPMI del iDRAC6 es compatible con el protocolo RMCP+. Consulte las especificaciones de IPMI 2.0 para obtener más información.

```
racadm config -g cfgIpmiLan -o
cfgIpmiEncryptionKey <clave>
```

donde <*clave*> es una clave de cifrado de 20 caracteres en un formato hexadecimal válido.

2 Configure la comunicación en serie en la LAN (SOL) con el comando siguiente:

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

NOTA: El nivel de privilegios mínimo de SOL de IPMI determina los privilegios mínimos que se requieren para activar la SOL de IPMI. Para obtener más información, consulte la especificación de IPMI 2.0.

a Actualice el nivel mínimo de privilegio de la SOL de IPMI con el comando siguiente:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege <nivel>
```

donde *<nivel>* es uno de los siguientes:

- 2 (**Usuario**)
- 3 (**Operador**)
- 4 (**Administrador**)

Por ejemplo, para definir los privilegios de IPMI como 2 (Usuario), introduzca el comando siguiente:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

NOTA: Para redirigir la consola de serie en la LAN, asegúrese de que la velocidad en baudios de la comunicación en serie en la LAN (SOL) sea idéntica a la velocidad en baudios del sistema administrado.

b Actualice la velocidad en baudios de la SOL de IPMI con el comando siguiente:

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <velocidad_en_baudios>
```

donde *<velocidad_en_baudios>* es 19200, 57600 ó 115200 bps.

Por ejemplo,

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

c Active la comunicación en serie en la LAN escribiendo el comando siguiente en el símbolo del sistema.

NOTA: Es posible activar o desactivar la SOL para cada usuario individual.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable 1 -i <id>
```

donde *<id>* es la identificación única del usuario.

Configuración del PEF

Puede configurar la acción que desea que el iDRAC6 ejecute ante cada alerta de plataforma. Tabla 13-3 muestra las acciones posibles y el valor para identificarlas en RACADM.

Tabla 13-3. Acción de sucesos de plataforma

Acción	Valor
Sin acción	0
Alimentación apagada	1
Reiniciar	2
Ciclo de encendido	3

Configure las acciones de filtro de sucesos de plataforma (PEF) con el comando siguiente:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction
-i <índice> <valor_de_acción>
```

donde <*índice*> es el índice de filtro de sucesos de plataforma (Tabla 5-7) y <*valor_de_acción*> es un valor de Tabla 13-3.

Por ejemplo, para hacer que el filtro de sucesos de plataforma reinicie el sistema y envíe una alerta de IPMI cuando se detecte un suceso crítico del procesador, introduzca el siguiente comando:

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction
-i 9 2
```

Configuración de la PET

1. Active las alertas globales con el comando siguiente:

   ```
   racadm config -g cfgIpmiLan -o
   cfgIpmiLanAlertEnable 1
   ```

2. Active la captura de sucesos de plataforma con el comando siguiente:

   ```
   racadm config -g cfgIpmiPet -o
   cfgIpmiPetAlertEnable -i <índice> <0|1>
   ```

donde <*índice*> es el índice de destino de la captura de sucesos de plataforma y `0` ó `1` desactiva o activa la captura de sucesos de plataforma, respectivamente.

Por ejemplo, para activar una PET con índice 4, introduzca el comando siguiente:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

3 Configure la política de captura de sucesos de plataforma con el comando siguiente:

```
racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i <índice>
<dirección_IP>
```

donde *índice* es el índice del destino de la captura de sucesos de plataforma y <*dirección_IP*> es la dirección IP de destino del sistema que recibe las alertas de sucesos de plataforma.

4 Configure la cadena de nombre de comunidad.

En el símbolo del sistema, introduzca:

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <nombre>
```

donde <*nombre*> es el nombre de comunidad de la captura de sucesos de plataforma.

Configuración de alertas por correo electrónico

1 Active las alertas globales con el comando siguiente:

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Active las alertas por correo electrónico con los comandos siguientes:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i <índice> <0|1>
```

donde <*índice*> es el índice del destino de correo electrónico y 0 desactiva la alerta por correo electrónico o 1 activa la alerta. El índice de destino de correo electrónico puede ser un valor de 1 a 4.

Por ejemplo, para activar un correo electrónico con índice 4, introduzca el comando siguiente:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 4 1
```

3 Configure los valores de correo electrónico con el comando siguiente:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress -i 1
<dirección_de_correo_electrónico>
```

donde 1 es el índice del destino del mensaje de correo electrónico y *<dirección_de_correo_electrónico>* es la dirección de correo electrónico de destino que recibe las alertas de sucesos de plataforma.

4 Para configurar el servidor SMTP de correo electrónico, introduzca el siguiente comando:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtpServerIpAddr <dirección IP del
servidor SMTP de correo electrónico>
```

5 Para configurar un mensaje personalizado, introduzca el comando siguiente:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertCustomMsg -i <índice>
<mensaje_personalizado>
```

donde *índice* es el índice del destino del mensaje de correo electrónico y *<mensaje_personalizado>* es el mensaje personalizado.

6 Si lo desea, pruebe la alerta configurada de correo electrónico con el comando siguiente:

```
racadm testemail -i <índice>
```

donde *<índice>* es el índice del destino de correo electrónico que va a probar.

Configuración del filtro de IP (Rango de IP)

La filtración de direcciones IP (o *Comprobación de rango de IP*) permite el acceso al iDRAC6 únicamente a los clientes o estaciones de administración cuyas direcciones IP estén dentro de un rango especificado por el usuario. Todas las demás solicitudes de inicio de sesión son denegadas.

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

- **cfgRacTuneIpRangeAddr**
- **cfgRacTuneIpRangeMask**

La propiedad **cfgRacTuneIpRangeMask** se aplica a la dirección IP entrante y a las propiedades **cfgRacTuneIpRangeAddr**. Si los resultados son idénticos, se permite que la petición de inicio de sesión entrante tenga acceso al iDRAC6. Los inicios de sesión provenientes de direcciones IP fuera de este rango recibirán un mensaje de error.

El inicio de sesión prosigue si el valor de la siguiente expresión es igual a cero:

```
cfgRacTuneIpRangeMask & (<dirección_IP_entrante> ^
cfgRacTuneIpRangeAddr)
```

donde `&` es el operador Y a nivel de bits de las cantidades y `^` es el operador O exclusivo a nivel de bits.

Consulte cfgRacTuning en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para obtener una lista completa de las propiedades cfgRacTuning.

Tabla 13-4. Propiedades del filtrado de direcciones IP (IPRange)

Propiedad	Descripción
cfgRacTuneIpRangeEnable	Activa la función de comprobación de rango de IP.
cfgRacTuneIpRangeAddr	Determina el patrón de bits de la dirección IP aceptable, en función de los números 1 de la máscara de subred. Esta propiedad se basa en el modo en bits y *AND* con **cfgRacTuneIpRangeMask** para determinar la parte superior de la dirección IP permitida. Se permite que inicie sesión cualquier dirección IP que contenga este patrón de bits en los bits superiores. Fallarán los inicios de sesión que provengan de las direcciones IP que estén fuera de este rango. Los valores predeterminados en cada propiedad permiten que el rango de direcciones de 192.168.1.0 a 192.168.1.255 inicien sesión.
cfgRacTuneIpRangeMask	Define las posiciones significativas de bit en la dirección IP. La máscara debe darse en forma de máscara de red, donde todos los bits más significativos son unos (1) con una sola transición total a ceros en los bits del orden inferior.

A continuación se presentan ejemplos de cómo utilizar RACADM local para configurar la filtración de IP.

NOTA: Ver "Uso de la interfaz de línea de comandos de RACADM" en la página 289 para obtener más información sobre RACADM y los comandos RACADM.

1 Los siguientes comandos de RACADM bloquean todas las direcciones IP, excepto la dirección 192.168.0.57:

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.255
```

2 Para restringir los inicios de sesión a un pequeño conjunto de cuatro direcciones IP adyacentes (por ejemplo, de 192.168.0.212 a 192.168.0.215), seleccione todo salvo los últimos dos bits de la máscara, según se muestra a continuación:

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.252
```

El último byte de la máscara de rango está establecido como 252, el equivalente decimal de 11111100b.

Directrices para el filtrado de IP

Utilice las directrices siguientes al activar el filtrado de IP:

- Compruebe que **cfgRacTuneIpRangeMask** esté configurado en forma de máscara de red, donde los bits más significativos son los números 1 (que definen la subred en la máscara) con una transición a sólo ceros en los bits de nivel inferior.
- Utilice la dirección base del rango deseado como el valor de **cfgRacTuneIpRangeAddr**. El valor binario de 32 bits de esta dirección debe tener ceros en todos los bits de orden inferior donde hay ceros en la máscara.

Configuración del bloqueo de IP

El bloqueo de IP detecta de forma dinámica cuando se presentan fallas de inicio de sesión provenientes de una dirección IP específica y bloquea (o impide) el inicio de sesión de dicha dirección en el iDRAC6 durante un lapso de tiempo predefinido.

Las funciones del bloqueo de IP incluyen:

- El número de fallas permitidas de inicio de sesión (**cfgRacTuneIpBlkFailcount**)
- El periodo en segundos durante el cual se deben presentar estas fallas (**cfgRacTuneIpBlkFailWindow**)

- La cantidad de tiempo en segundos durante el que se impide que la dirección IP bloqueada establezca una sesión después de haber excedido el número de fallas permitidas (**cfgRacTuneIpBlkPenaltyTime**)

Conforme se acumulan las fallas de inicio de sesión provenientes de una dirección IP específica, un contador interno lleva registro de las mismas. Cuando el usuario inicia sesión satisfactoriamente, el historial de intentos fallidos se borra y el contador interno se restablece.

NOTA: Cuando se rechazan los intentos de inicio de sesión provenientes de la dirección IP cliente, algunos clientes de SSH pueden mostrar el siguiente mensaje: `Identificación de intercambio de SSH: El host remoto cerró la conexión.`

Consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals** para obtener una lista completa de las propiedades **cfgRacTune**.

La Tabla 13-5 muestra una lista de los parámetros definidos por el usuario.

Tabla 13-5. Propiedades de restricción (Bloqueo de IP) de reintentos de inicio de sesión

Propiedad	Definición
cfgRacTuneIpBlkEnable	Activa la función de bloqueo de IP. Cuando se presenten fallas consecutivas (**cfgRacTuneIpBlkFailCount**) provenientes de una única dirección IP dentro de un lapso de tiempo específico (**cfgRacTuneIpBlkFailWindow**), todos los intentos posteriores de establecimiento de sesión que provengan de dicha dirección serán rechazados durante un periodo de tiempo determinado (**cfgRacTuneIpBlkPenaltyTime**).
cfgRacTuneIpBlkFailCount	Establece el número de intentos fallidos de inicio de sesión provenientes de una dirección IP antes de rechazar los intentos de inicio de sesión.
cfgRacTuneIpBlkFailWindow	El periodo en segundos durante el cual se cuentan los intentos fallidos. Cuando los intentos fallidos superan este límite, se eliminan del contador.

Tabla 13-5. Propiedades de restricción (Bloqueo de IP) de reintentos de inicio de sesión *(continuación)*

Propiedad	Definición
cfgRacTuneIpBlkPenaltyTime	Define el periodo en segundos dentro del cual se rechazarán los intentos de inicio de sesión que provengan de una dirección IP con fallas excesivas.

Activación del bloqueo de IP

El ejemplo siguiente impide a una dirección IP cliente establecer una sesión durante cinco minutos si dicho cliente ha fallado cinco intentos de inicio de sesión en un periodo de un minuto.

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 300
```

El ejemplo siguiente impide más de tres intentos fallidos dentro de un minuto e impide los intentos de inicio de sesión adicionales durante una hora.

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

Configuración de los servicios de Telnet y SSH del iDRAC6 por medio de RACADM local

La consola de Telnet/SSH se puede configurar de manera local (en el servidor administrado) con los comandos RACADM.

NOTA: Se debe tener permiso de **Configurar el iDRAC6** para ejecutar los comandos en esta sección.

NOTA: Cuando usted reconfigura los valores de Telnet o SSH en el iDRAC6, todas las sesiones actuales se terminan sin aviso.

Para activar Telnet y SSH desde RACADM local, inicie sesión en el servidor administrado e introduzca los siguientes comandos en el símbolo del sistema:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Para desactivar el servicio Telnet o SSH, cambie el valor de `1` a `0`:

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 0
racadm config -g cfgSerial -o cfgSerialSshEnable 0
```

Introduzca el siguiente comando para cambiar el número de puerto de Telnet en el iDRAC6:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
<número del nuevo puerto>
```

Por ejemplo, para cambiar el puerto Telnet del valor predeterminado 23 a 8022, introduzca este comando:

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort
8022
```

Para ver una lista completa de los comandos disponibles de la CLI de RACADM, ver "Uso de la interfaz de línea de comandos de RACADM" en la página 289.

RACADM SSH/Telnet y remoto

RACADM remoto es una utilidad en el cliente que puede ejecutarse desde una estación de administración a través de la interfaz de red fuera de banda. Se proporciona una opción de capacidad remota (**-r**) que le permite conectarse al sistema administrado y ejecutar subcomandos de RACADM desde una consola remota o una estación de administración. Para usar la capacidad remota, necesita un nombre de usuario válido (opción **-u**) y una contraseña (opción **-p**), así como la dirección IP del iDRAC6. RACADM SSH/Telnet se utiliza para hacer referencia al uso del comando de RACADM desde un símbolo del sistema SSH o Telnet.

La cantidad máxima de sesiones simultáneas de RACADM remoto es cuatro. Estas sesiones son independientes y adicionales a las sesiones de Telnet y SSH. El iDRAC6 puede admitir simultáneamente cuatro sesiones SSH y cuatro sesiones de Telnet, además de las cuatro sesiones de RACADM.

NOTA: Configure la dirección IP en el iDRAC6 antes de usar la capacidad remota de RACADM.

NOTA: Si el sistema desde el que está accediendo al sistema remoto no tiene un certificado de iDRAC6 en el almacén predeterminado de certificados, aparece un mensaje al escribir un comando de RACADM.

```
Alerta de seguridad: el certificado no es válido;
el nombre que aparece en el certificado no es
válido o no coincide con el nombre del sitio

Ejecución continua. Utilice la opción -S para que
racadm detenga la ejecución al producirse errores
relacionados con certificados.
```

RACADM continúa ejecutando el comando. No obstante, si utiliza la opción `–S`, RACADM detendrá la ejecución del comando y mostrará el siguiente mensaje:

```
Alerta de seguridad: el certificado no es válido;
el nombre que aparece en el certificado no es
válido o no coincide con el nombre del sitio

Racadm detiene la ejecución del comando.

ERROR: no es posible establecer conexión con el
iDRAC6 en la dirección IP especificada
```

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

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

o

```
racadm sslcertdownload -t <tipo>
[-f <nombredearchivo>]
```

Uso de RACADM remoto

`racadm -r <dirección IP del iDRAC6> -u <nombre de usuario> -p <contraseña> <subcomando> <opciones del subcomando>`

`racadm -i -r <dirección IP del iDRAC6> <subcomando> <opciones del subcomando>`

Por ejemplo,

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

```
racadm -i -r 192.168.0.120 getsysinfo
```

Si el número de puerto HTTPS del iDRAC6 se ha cambiado a un puerto personalizado diferente al predeterminado (443), se debe utilizar la siguiente sintaxis:

`racadm -r <dirección IP del iDRAC6>:<puerto> -u <nombre_de_usuario> -p <contraseña> <subcomando> <opciones del subcomando>`

`racadm -i -r <dirección IP del iDRAC6>:<puerto> <subcomando> <opciones del subcomando>`

Opciones de RACADM remoto

La Tabla 13-6 muestra las opciones para los comandos de RACADM remoto.

Tabla 13-6. Opciones de comandos de RACADM

Opción	Descripción
-r <*dirección IP del RAC*> **-r** <*dirección IP del RAC*>:<*número de puerto*>	Especifica la dirección IP remota del controlador. Utilice <*número de puerto*> si el número de puerto del iDRAC6 no es el puerto predeterminado (443)
-i	Indica a RACADM que pregunte interactivamente al usuario el nombre de usuario y la contraseña.
-u <*Nombre de usuario*>	Especifica el nombre de usuario que se usa para autentificar la transacción del comando. Si se usa la opción **-u**, se debe usar la opción **-p**, y la opción **-i** (interactiva) no se permite.
-p <*contraseña*>	Especifica la contraseña usada para autentificar la transacción del comando. Si se usa la opción **-p**, la opción **-i** no se permite.
-S	Indica que RACADM debe verificar si existen errores por certificados no válidos. RACADM detiene la ejecución del comando y muestra un mensaje de error si detecta un certificado no válido.

NOTA: No se recomienda el uso de otros caracteres diferentes a los caracteres que no son alfanuméricos como, por ejemplo, $, %, <, >, | etc. en los argumentos de comando de RACADM. El uso de los mismos podría provocar un comportamiento inesperado.

Uso de un archivo de configuración de iDRAC6

El archivo de configuración de iDRAC6 es un archivo de texto que contiene una representación de los valores en la base de datos de iDRAC6. Puede utilizar el subcomando **getconfig** de RACADM para generar un archivo de configuración que contenga los valores actuales del iDRAC6. Puede editar entonces el archivo y utilizar el subcomando **config -f** de RACADM para volver a cargar el archivo en el iDRAC6 o para copiar la configuración a otros iDRAC6.

Creación de un archivo de configuración del iDRAC6

El archivo de configuración es un archivo de texto simple. Se puede utilizar cualquier nombre de archivo válido; sin embargo, la convención recomendada es la extensión de archivo **.cfg**.

El archivo de configuración se puede:

- Crear con un editor de textos
- Obtenerse del iDRAC6 con el subcomando **getconfig** de RACADM
- Obtenerse del iDRAC6 con el subcomando **getconfig** de RACADM y después editarse

Para obtener un archivo de configuración con el comando **getconfig** de RACADM, introduzca el siguiente comando:

```
racadm -r <remote iDRAC6 IP> -u <user> -p <password>
getconfig -f myconfig.cfg
```

Este comando crea el archivo **myconfig.cfg** en el directorio actual.

Sintaxis del archivo de configuración

NOTA: Modifique el archivo de configuración con un editor de textos sin formato, como el **Bloc de notas** en Windows o **vi** en Linux. La utilidad **racadm** analiza únicamente el texto ASCII. Los formatos confunden al analizador y pueden dañar la base de datos del iDRAC6.

Esta sección describe el formato del archivo de configuración.

- Las líneas que comienzan con # son comentarios.

  Un comentario *debe* comenzar en la primera columna de la línea. Un carácter # que esté en cualquier otra columna será tratado como carácter # normal.

  Ejemplo:

  ```
  #

  # Esto es un comentario

  [cfgUserAdmin]

  cfgUserAdminPrivilege=4
  ```

- Todas las anotaciones de grupo deben estar encerradas en los caracteres *[* y *]*.

  El carácter inicial *[* que denota un nombre de grupo *debe* comenzar en la columna uno. Este nombre de grupo *se debe* especificar antes que cualquiera de los objetos en el grupo. Los objetos que no tienen un nombre de grupo asociado producirán un error. Los datos de la configuración se organizan en grupos según se define en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

  El siguiente ejemplo muestra un nombre de grupo, el objeto y el valor de propiedad del objeto.

  Ejemplo:

  `[cfgLanNetworking]` (*nombre de grupo*)

  `cfgNicIpAddress=192.168.1.1` (*nombre de objeto*)

- Todos los parámetros se especifican como pares *objeto=valor* sin espacio en blanco entre el objeto, el signo "=" y el valor.

  El espacio en blanco que se incluye después del valor se ignora. El espacio en blanco dentro de una cadena de valores no se modifica. Todo carácter a la derecha del signo = se toma tal cual es (por ejemplo, un segundo = o un #, *[*, *]*, etc.).

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

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

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

  `[cfgUserAdmin]`

  `cfgUserAdminIndex=11`

- Si el analizador encuentra un grupo indexado, el índice del grupo se utiliza como ancla. Todas las modificaciones a los objetos dentro del grupo indexado se asocian también con el valor del índice.

Por ejemplo,

```
[cfgUserAdmin]

# cfgUserAdminIndex=11

cfgUserAdminUserName=

# cfgUserAdminPassword=******** (Sólo lectura)

cfgUserAdminEnable=0

cfgUserAdminPrivilege=0x00000000

cfgUserAdminIpmiLanPrivilege=15

cfgUserAdminIpmiSerialPrivilege=15

cfgUserAdminSolEnable=0
```

- Los índices son de sólo lectura y no se pueden modificar. Los objetos del grupo indexado están vinculados al índice bajo el que se enumeran y cualquier configuración válida del valor del objeto se aplica únicamente a ese índice en particular.
- Hay un conjunto predefinido de índices disponible para cada grupo indexado. Para obtener más información, consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Modificación de la dirección IP del iDRAC6 en un archivo de configuración

Cuando modifique la dirección IP del iDRAC6 en el archivo de configuración, elimine todas las anotaciones de <*variable*>=<*valor*> innecesarias. Sólo la etiqueta variable real del grupo con "[" y "]" permanecerá, incluyendo las dos anotaciones <*variable*>=<*valor*> relacionadas con el cambio de la dirección IP.

Por ejemplo,

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

```
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Este archivo será actualizado de la siguiente manera:

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

Carga del archivo de configuración en el iDRAC6

El comando `racadm config -f <nombre_de_archivo>` analiza el archivo de configuración para verificar que el grupo y los nombres de objeto válidos estén presentes y que se cumpla con las reglas de la sintaxis. Si el archivo no tiene errores, el comando actualizará la base de datos del iDRAC6 con el contenido del archivo.

NOTA: Para verificar únicamente la sintaxis y no actualizar la base de datos del iDRAC6, agregue la opción **-c** al subcomando **config**.

Los errores dentro del archivo de configuración se señalan con el número de línea y un mensaje que explica el problema. Usted deberá corregir todos los errores antes de que el archivo de configuración actualice al iDRAC6.

NOTA: Utilice el subcomando **racresetcfg** para restablecer la base de datos y la configuración de la tarjeta de interfaz de red del iDRAC6 a la configuración predeterminada original y para eliminar a todos los usuarios y configuraciones de usuario. Aunque el usuario raíz está disponible, también se restablecerá la configuración predeterminada de los demás usuarios.

Antes de ejecutar el comando `racadm config -f <nombre_de_archivo>`, puede ejecutar el subcomando `racresetcfg` para restablecer la configuración predeterminada del iDRAC6. Asegúrese de que el archivo que se va a cargar incluya todos los objetos, usuarios, índices y otros parámetros deseados.

Para actualizar el iDRAC6 con el archivo de configuración, ejecute el siguiente comando:

```
racadm -r <remote iDRAC6 IP> -u <user> -p <password>
config -f myconfig.cfg
```

Después de que el comando ha terminado, usted puede ejecutar el subcomando **getconfig** de RACADM para confirmar que la actualización fue satisfactoria.

Configuración de varios iDRAC6

A través de un archivo de configuración, usted puede configurar otros iDRAC6 con propiedades idénticas. Siga estos pasos para configurar varios iDRAC6:

1. Cree el archivo de configuración del iDRAC6 cuyos valores desea copiar en los demás. Introduzca el comando siguiente:

   ```
   racadm -r <remote iDRAC6 IP> -u <user> -p
   <password> getconfig -f <filename>
   ```

   donde <*nombre de archivo*> es el nombre de un archivo para guardar las propiedades del iDRAC6, como **myconfig.cfg**.

   El ejemplo a continuación muestra cómo es posible utilizar comandos de RACADM remoto para configurar varios iDRAC6. Cree un archivo de procesamiento en lote en la estación de administración y ejecute los comandos de RACADM remoto desde el archivo de proceso por lotes.

   Por ejemplo,

   ```
   racadm -r <Server IP 1> -u <user> -p <password>
   config -f myconfig.cfg

   racadm -r <Server IP 2> -u <user> -p <password>
   config -f myconfig.cfg

   ...
   ```

   Ver “Creación de un archivo de configuración del iDRAC6” en la página 315 para obtener más información.

NOTA: Algunos archivos de configuración contienen información exclusiva del iDRAC6 (como la dirección IP estática) que debe modificarse antes de exportar el archivo a otros iDRAC6.

2 Modifique el archivo de configuración que ha creado en el paso anterior y quite o marque como comentarios los valores que *no desea* reproducir.

3 Copie el archivo de configuración modificado en una unidad de red donde esté disponible para cada servidor administrado cuyo iDRAC6 desea configurar.

4 Para cada iDRAC6 que desea configurar:

   a Inicie sesión en el servidor administrado y abra un símbolo del sistema.

   b Si desea cambiar la configuración predeterminada del iDRAC6, introduzca el comando siguiente:

   ```
   racadm racresetcfg
   ```

   c Cargue el archivo de configuración en el iDRAC6 con el comando siguiente:

   ```
   racadm -r <remote iDRAC6 IP> -u <user> -p
   <password> config -f <filename>
   ```

   donde <*nombre_de_archivo*> es el nombre del archivo de configuración que ha creado. Incluya la ruta de acceso completa si el archivo no está en el directorio de trabajo.

   d Restablezca el iDRAC6 que se configuró por medio del comando siguiente:

   ```
   racadm racreset
   ```

14

Supervisión y administración de la alimentación

Los sistemas Dell PowerEdge incorporan muchas características nuevas y mejoradas para la administración de la alimentación. El diseño de toda la plataforma, desde el hardware al firmware, pasando por el software de administración de sistemas, está orientado a la eficacia energética, y a la supervisión y administración de energía.

NOTA: La lógica de administración de la alimentación del iDRAC6 utiliza un dispositivo lógico programable complejo, denominado CPLD por sus siglas en inglés, que se encuentra en el servidor Blade. Algunas plataformas también admiten dispositivos CPLD ampliados. Las actualizaciones de los dispositivos CPLD están disponibles en el sitio web del servicio de asistencia Dell Support en **support.dell.com**, en las secciones **Firmware del sistema** o **Placa base**.
Se recomienda actualizar el servidor blade con la versión más reciente de firmware del CPLD. La versión actual del firmware del CPLD y la ampliada (para determinadas plataformas) se muestra en la interfaz gráfica del usuario de web del iDRAC6.

Los sistemas Dell PowerEdge proporcionan muchas funciones para supervisar y administrar la alimentación:

- **Supervisión de alimentación:** El iDRAC6 recopila un historial de mediciones energéticas y calcula promedios de ejecución, picos y situaciones similares. Con la interfaz web del iDRAC6 se puede ver esta información en la pantalla **Supervisión de alimentación**. También se puede visualizar esta información en forma de gráficos haciendo un clic en **Mostrar gráfico** en el extremo inferior de la pantalla **Supervisión de alimentación**. Para obtener más información, ver "Supervisión de alimentación" en la página 322.
- **Presupuesto de alimentación:** durante el inicio, un inventario del sistema permite calcular un presupuesto de alimentación de la configuración actual. Ver "Presupuesto de alimentación" en la página 325 para obtener más información.
- **Control de alimentación:** el iDRAC6 permite realizar varias acciones de administración de la alimentación en el sistema administrado de manera remota. Ver "Power Control" en la página 330 para obtener más información.

Configuración y administración de la alimentación

Se puede usar la interfaz web del iDRAC6 y la interfaz de línea de comandos (CLI) de RACADM para administrar y configurar los controles de alimentación en el sistema Dell PowerEdge. Específicamente, puede:

- Ver el estado de alimentación del servidor. Vea la "Ver la supervisión de alimentación" en la página 323.
- Ver la información de presupuesto de alimentación del servidor, incluido el potencial consumo de alimentación mínimo y máximo. Vea la "Ver el presupuesto de alimentación" en la página 327.
- Ver el umbral del presupuesto de alimentación del servidor. Vea la "Umbral de presupuesto de alimentación" en la página 328.
- Ver la alimentación asignada a las tarjetas de expansión PCIe del servidor. Vea la "Cómo ver y modificar la asignación de alimentación de PCIe" en la página 329.
- Ejecutar operaciones de control de alimentación en el servidor (por ejemplo, encendido, apagado, restablecimiento del sistema, ciclo de encendido y apagado ordenado). Vea la "Ejecución de operaciones de control de alimentación en el servidor" en la página 331.

Supervisión de alimentación

El iDRAC6 supervisa el consumo de alimentación en los servidores Dell PowerEdge en forma continua. El iDRAC6 calcula los siguientes valores de alimentación y proporciona la información a través de su interfaz web o de línea de comandos de RACADM:

- Potencia acumulada del sistema
- Alimentación y amperaje picos del sistema
- Consumo de alimentación promedio, mínimo y máximo
- Consumo de alimentación (también se puede ver en gráficos en la interfaz web)
- Fechas y horas de alimentación máx. y mín.

Ver la supervisión de alimentación

Cómo utilizar la interfaz web

Para ver la información de supervisión de alimentación:

1. Inicie sesión en la interfaz web del iDRAC6.
2. En el árbol del sistema, seleccione **Supervisión de alimentación**.

   Aparece la pantalla **Supervisión de alimentación**, con la siguiente información:

Supervisión de alimentación

- **Estado**: una **marca de verificación verde** indica que el estado de la alimentación es normal, **Advertencia** indica que se ha emitido una alerta de aviso y **Grave** indica que se ha emitido una alerta de falla.
- **Nombre de la sonda**: indica el nombre del sensor.
- **Lectura**: indica el vataje informado por la sonda.
- **Umbral de advertencia**: muestra el consumo de energía aceptable (en vatios y BTU/h) recomendados para el funcionamiento del sistema. El consumo de energía que exceda este valor dará como resultado la aparición de eventos de aviso y regulaciones de la CPU.
- **Umbral de falla**: muestra el consumo de energía aceptable más alto (en vatios y BTU/h) requerido para el funcionamiento del sistema. El consumo de energía que exceda este valor dará como resultado la aparición de eventos de error y críticos, lo cual apagará el servidor Blade.

Amperaje

- **Ubicación**: muestra el nombre del sensor de la placa del sistema.
- **Lectura**: el consumo actual de corriente alterna, en amperios

Estadísticas de seguimiento de alimentación y estadísticas pico

- **Estadística:**
  - **Potencia acumulada del sistema** muestra el consumo de energía acumulada actual (en kWh) del servidor. El valor representa la alimentación total utilizada por el sistema. Puede restablecer este valor a 0 al hacer clic en **Restablecer**, ubicada al final de la fila.

– **Alimentación pico del sistema** especifica el valor pico del sistema, en vatios de corriente alterna.

– **Amperaje pico del sistema** especifica el amperaje pico del sistema. El valor pico es el valor más alto registrado entre la **hora inicial de medición** y ahora. La hora pico fue el momento en que ocurrió el valor pico. Haga clic en **Restablecer** al final de la fila de la tabla para volver a establecer el valor instantáneo actual (el cual no será 0 si el servidor está en funcionamiento). Al seleccionar el restablecimiento, también se restablecerá la hora inicial de medición y se fijará la hora actual.

– La **Hora inicial de medición** muestra la fecha y hora registradas cuando se borró por última vez el valor de consumo de energía del sistema y comenzó el nuevo ciclo de mediciones. Para las estadísticas **Potencia acumulada del sistema**, **Amperaje pico del sistema** y **Alimentación pico del sistema**, los valores pico, al restablecerse, mostrarán inmediatamente el valor instantáneo actual.

– La **Hora actual de medición** para la **Potencia acumulada del sistema** muestra la fecha y hora en las que se calculó el consumo de energía del sistema para su visualización. Para el **Amperaje pico del sistema** y la **Alimentación pico del sistema**, los campos de **Hora pico** muestran la hora en que tuvieron lugar dichos picos.

– **Lectura**: el valor de la estadística correspondiente: **Potencia acumulada del sistema**, **Alimentación pico del sistema** y **Amperaje pico del sistema** desde que se inició el contador.

NOTA: Se mantienen estadísticas de seguimiento de alimentación luego de todos los restablecimientos del sistema. De este modo se refleja toda la actividad en el intervalo entre la hora de inicio y la actual. Los valores de alimentación que se muestran en la tabla de consumo de alimentación son promedios acumulados en el intervalo de tiempo respectivo (minuto, hora, día y semana últimos). Debido a que los intervalos de tiempo de inicio a fin pueden ser distintos de aquellos de las estadísticas de seguimiento de alimentación, los valores máximos de alimentación (máximos en vatios en comparación con consumo máximo de energía) pueden ser distintos.

Power Consumption

- **Consumo de alimentación promedio**: promedio sobre minuto, hora, día y semana anteriores.
- **Consumo de alimentación máximo y Consumo de alimentación mínimo:** el consumo de alimentación máximo y mínimo observado dentro de un intervalo de tiempo determinado.
- **Fecha y hora de alimentación máxima** y **Fecha y hora de alimentación mínima**: el momento (minuto, hora, día y semana) en el que ocurrió el consumo de alimentación mínimo y máximo.

Mostrar gráfica

Haga clic en **Mostrar gráfico** para ver los gráficos con el consumo de alimentación del iDRAC6 en vatios durante la última hora, las últimas 24 horas, tres días y una semana. Utilice el menú desplegable que se encuentra por encima del gráfico para seleccionar el período de tiempo.

NOTA: Cada uno de los puntos de información de la gráfica representa el promedio de lecturas en un lapso de 5 minutos. Como resultado, es posible que la gráfica no refleje fluctuaciones breves de potencia ni de consumo.

Presupuesto de alimentación

La pantalla **Presupuesto de alimentación** muestra los límites de los umbrales de alimentación, los cuales cubren el rango de consumo, en corriente alterna, que presentará al centro de datos un sistema con una gran carga de trabajo.

Antes de que un servidor se encienda, el iDRAC6 le proporciona al CMC los requisitos de envolvente de potencia. El envolvente de potencia proporcionado a CMC por medio del iDRAC antes de que el sistema se encienda es superior a la potencia actual que el servidor blade puede consumir. El envolvente de potencia se calcula en función a la información de inventario de hardware limitada. El iDRAC6 puede solicitar una envolvente de potencia inferior una vez energizado el servidor, de acuerdo con la alimentación real consumida por éste. Si el consumo de energía aumenta con el tiempo y el consumo del servidor se acerca a su asignación máxima, el iDRAC6 puede requerir un aumento del consumo de energía máximo potencial, lo que incrementa la envolvente de potencia. El iDRAC6 sólo aumenta el requisito de consumo de alimentación máximo potencial para el CMC y no requiere un mínimo de alimentación potencial inferior si el consumo disminuye. iDRAC continuará solicitando más alimentación si el consumo de energía excede la alimentación asignada por CMC.

Una vez que el sistema está encendido e inicializado, iDRAC calcula un nuevo envolvente de potencia que está basado en la configuración actual del servidor blade. El servidor blade continuará encendido incluso si CMC falla a la hora de asignar una nueva solicitud de alimentación.

El CMC recupera toda alimentación sin utilizar de los servidores de menor prioridad y luego la asigna a un servidor o módulo de infraestructura de mayor prioridad.

Si no se ha asignado suficiente alimentación, el servidor blade no se enciende. Si el servidor blade tiene asignada suficiente alimentación, el iDRAC enciende la alimentación del sistema.

El iDRAC6 también admite la asignación de alimentación a las tarjetas de expansión PCIe para determinadas plataformas. Se puede cambiar la asignación de alimentación a las tarjetas de expansión PCIe instaladas en las ranuras de expansión del servidor. Se pueden instalar dos tarjetas PCIe en determinadas plataformas. El iDRAC ajusta en forma dinámica la potencia máxima acercándola al requisito real del sistema para el servidor blade, agrega la alimentación asignada a la ranura de la tarjeta de expansión y le solicita al CMC la alimentación total. Para obtener más información sobre tarjetas de expansión, consulte el *Manual del propietario del hardware* disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**. Para obtener información acerca de cómo modificar la asignación de alimentación de las PCIe, ver "Cómo ver y modificar la asignación de alimentación de PCIe" en la página 329.

Después de encenderse el servidor blade, el BIOS inicia y detecta el consumo real de alimentación de las tarjetas de expansión PCIe. Esto ocurre durante la POST. El iDRAC conserva el valor utilizado en la fase de preinicialización para las tarjetas de expansión si ambas tarjetas están presentes. Una vez obtenido el valor actualizado en base a las tarjetas PCIe actualmente instaladas, el iDRAC combina ese valor con el consumo estimado de alimentación de la tarjeta de expansión e informa un nuevo valor de alimentación para el blade general. Si el CMC no asigna suficiente alimentación, el iDRAC apagará el servidor blade. Si el CMC asigna suficiente alimentación, se permite a BIOS que continúe iniciando y el servidor puede encenderse.

Por ejemplo: Si 500 W es el valor que el iDRAC supone durante la preinicialización, se usará ese valor salvo que se determine otro diferente en la asignación de la ranura de expansión de la PCIe. Si se determina un valor diferente, siempre se lo usará durante la inicialización. El valor se preserva a través de los ciclos de encendido de corriente alterna. El valor de entrada se compara entonces con el número de tarjetas instaladas cuando el sistema alcanza el POST.

Ver el presupuesto de alimentación

El servidor proporciona una descripción general del estado del presupuesto de alimentación del subsistema de alimentación en la pantalla **Presupuesto de alimentación**.

Cómo utilizar la interfaz web

NOTA: Para realizar acciones de administración de energía, se debe contar con privilegios de **Administrador**.

1. Inicie sesión en la interfaz web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema**.
3. Haga clic en la ficha **Administración de la alimentación** y luego en **Presupuesto de alimentación**.

   Aparecerá la pantalla **Presupuesto de alimentación**.

La tabla **Información sobre el presupuesto de alimentación** muestra los límites mínimo y máximo de los umbrales de alimentación para la configuración actual del sistema. Estos cubren el rango de consumo de corriente alterna que presentará al centro de datos un sistema de umbrales con una gran carga de trabajo.

- El **consumo de alimentación potencial mínimo** representa el valor más bajo del umbral de presupuesto de alimentación.
- El **consumo de alimentación potencial máximo** representa el valor más alto del umbral de presupuesto de alimentación. Este valor es también el consumo de alimentación máximo absoluto de la configuración actual del sistema.

Cómo utilizar de RACADM

En un servidor administrado, abra una interfaz de línea de comandos e introduzca:

```
racadm getconfig -g cfgServerPower
```

NOTA: Para obtener más información sobre cfgServerPower, incluidos los detalles de salida, consulte cfgServerPower en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Umbral de presupuesto de alimentación

El umbral del presupuesto de alimentación, si está activado, aplica los límites de alimentación para el sistema. El rendimiento del sistema se ajusta en forma dinámica a fin de mantener el consumo de alimentación cerca del umbral determinado.

El consumo de alimentación real puede ser menor en cargas de trabajo más livianas y puede exceder el umbral de forma momentánea hasta completar los ajustes de rendimiento.

NOTA: El umbral del presupuesto de alimentación es de sólo lectura y no es posible activarlo ni configurarlo en el iDRAC6.

Cómo utilizar la interfaz web

1. Inicie sesión en la interfaz web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema**.
3. Haga clic en la ficha **Administración de la alimentación** y luego en **Presupuesto de alimentación**.

   Aparecerá la pantalla **Presupuesto de alimentación**. La tabla del **Umbral del presupuesto de alimentación** muestra la siguiente información relativa al límite de alimentación del sistema:

   - **Activado** indica si el sistema aplica el umbral del presupuesto de alimentación.
   - **Umbral en vatios** y **Umbral en BTU/h** muestran el límite en vatios de corriente alterna y BTU/h, respectivamente.
   - **Umbral en porcentaje (del máximo)** muestra el porcentaje del rango de límites de alimentación.

Cómo utilizar de RACADM

Para ver los datos del umbral del presupuesto de alimentación de la RACADM remota, en el servidor administrado, abra una interfaz de línea de comandos e introduzca:

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapWatts
```

Informa *<valor límite de alimentación en vatios de corriente alterna>*

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapBTUhr
```

Informa *<valor límite de alimentación en BTU/h>*

```
racadm getconfig -g cfgServerPower -o
cfgServerPowerCapPercent
```

Informa *<valor límite de alimentación en %>*

NOTA: Para obtener más información sobre cfgServerPower, incluidos los detalles de salida, consulte cfgServerPower en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Cómo ver y modificar la asignación de alimentación de PCIe

La asignación de alimentación de PCIe permite ver y cambiar la alimentación máxima asignada a las tarjetas de expansión PCIe. La alimentación asignada debería estar entre 100 W y 500 W. Si se asigna demasiada alimentación es posible que el servidor blade no se inicie o que otros servidores blade del chasis no puedan iniciarse. Si la tarjeta de expansión PCIe consume más alimentación que la asignada, el servidor blade se apagará. Si se modifica la asignación de alimentación de las PCIe, el nuevo valor de asignación de alimentación se usa cuando el sistema se inicia.

NOTA: La información de asignación de alimentación de las PCIe no se aplica a todas las plataformas y no se mostrará para las plataformas donde no se aplica.

NOTA: Debe tener privilegios de administrador (Configurar el iDRAC y ejecutar comandos de control del servidor) para editar el valor de la asignación de alimentación de las PCIe.

Cómo utilizar la interfaz web

1. Inicie sesión en la interfaz web del iDRAC6.
2. En el árbol del sistema, seleccione **Sistema**.
3. Haga clic en la ficha **Administración de la alimentación** y luego en **Presupuesto de alimentación**. La tabla **Asignación de alimentación de las PCIe** muestra la asignación actual de alimentación en el campo **Umbral de alimentación en vatios**.

4 Introduzca el valor necesario o haga clic en **Valor predeterminado** para especificar un valor predeterminado. Los valores válidos son 100 W - 500 W. El valor predeterminado es 500 W.

5 Haga clic en **Aplicar** para guardar el valor nuevo. El valor nuevo se usa cuando el sistema se inicia.

Cómo utilizar de RACADM

Para ver la alimentación actualmente asignada a las tarjetas de expansión PCIe con RACADM remota, en el sistema remoto, abra un símbolo del sistema e introduzca el comando siguiente:

```
racadm -r <idracip> -u <user> -p <password> config -g
cfgServerPower -o cfgServerPowerPCIeAllocation
```

Ofrece <*valor máximo de alimentación expresado en vatios o en BTU/h*>. El valor predeterminado es 500 W.

Para cambiar el valor de asignación de alimentación (por ejemplo: 250 W):

```
racadm -r <idracip> -u <user> -p <password> config -g
cfgServerPower -o cfgServerPowerPCIeAllocation 250
```

Determina el valor en 250 W

NOTA: El objeto cfgServerPowerPCIeAllocation sólo es admitido en RACADM remota y no en RACADM local.

NOTA: Para obtener más información, consulte cfgServerPowerPCIeAllocation en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Power Control

El iDRAC6 le permite realizar las siguientes acciones de manera remota: Encendido, apagado, reinicio, apagado ordenado, interrupción no enmascarable (NMI) o ciclo de encendido. Utilice la pantalla **Control de alimentación** para realizar un apagado ordenado por medio del sistema operativo al reiniciar, encender y apagar el sistema.

Ejecución de operaciones de control de alimentación en el servidor

NOTA: Para realizar acciones de administración de la alimentación, debe contar con privilegios de **Administrador**.

El iDRAC6 le permite realizar de manera remota las siguientes acciones: encendido, reinicio, apagado ordenado, interrupción no enmascarable (NMI) o ciclo de encendido.

Cómo utilizar la interfaz web

1. Inicie sesión en la interfaz web del iDRAC6.
2. Seleccione **Sistema** en el árbol del sistema.
3. Haga clic en la ficha **Administración de alimentación**.

   Aparece la pantalla **Control de alimentación**.
4. Seleccione una de las siguientes **Operaciones de control de alimentación** haciendo clic en el botón de radio:
   - **Encender el sistema** enciende el servidor (equivalente a presionar el botón de encendido cuando el servidor está apagado). Esta opción se desactivará si el sistema ya está encendido.
   - **Apagar el sistema** apaga el servidor. Esta acción está desactivada si el sistema ya está apagado.
   - **NMI (interrupción no enmascarable)** genera una NMI para interrumpir la operación del sistema. Una NMI envía una interrupción de alto nivel al sistema operativo, lo cual hace que el sistema detenga la operación para permitir la ejecución de actividades fundamentales de diagnóstico o solución de problemas. Esta acción está desactivada si el sistema ya está apagado.
   - **Apagado ordenado** intenta cerrar el sistema operativo y luego apaga el sistema. Para efectuar un apagado ordenado, es necesario contar con un sistema operativo con Interfaz de energía y configuración avanzada (ACPI), lo cual permite la administración de la alimentación dirigida por el sistema. Esta acción está desactivada si el sistema ya está apagado.
   - **Restablecer el sistema (reinicio mediante sistema operativo)** reinicia el sistema sin apagarlo. Esta acción está desactivada si el sistema ya está apagado.

– **Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)** apaga el sistema y luego lo reinicia. Esta acción está desactivada si el sistema ya está apagado.

5 Haga clic en **Aplicar**.

Aparece un cuadro de diálogo solicitando confirmación.

6 Haga clic en **Aceptar** para ejecutar la acción de administración de la alimentación que ha seleccionado.

Cómo utilizar de RACADM

Para realizar acciones de alimentación desde RACADM local, introduzca el siguiente texto en el símbolo del sistema:

```
racadm serveraction <action>
```

donde `<action>` es `encendido`, `apagado`, `ciclo de encendido`, `apagado no ordenado` o estado de alimentación.

NOTA: Para obtener más información sobre serveraction, incluidos los detalles de salida, consulte serveraction en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

15

Uso de la interfaz de línea de comandos SM-C LP de iDRAC6 Enterprise

Esta sección proporciona información acerca del Protocolo de línea de comandos de administración de servidor (SM-CLP) del Grupo de trabajo de administración de servidor (SMWG) que está incorporado en el iDRAC6.

NOTA: Esta sección supone que el lector está familiarizado con la iniciativa SMASH (Arquitectura de administración de sistemas para hardware de servidor) y con las especificaciones de SM-CLP de SMWG. Para obtener más información acerca de estas especificaciones, visite el sitio web del Grupo de trabajo de administración distribuida (DMTF, por sus siglas en inglés) en **dmtf.org**.

El SM-CLP de iDRAC6 es un protocolo impulsado por DMTF y SMWG para proporcionar estándares para las implementaciones de la interfaz de línea de comandos (CLI) para administración de sistemas. Se están realizando muchos esfuerzos para obtener una arquitectura SMASH definida como punto de partida para un conjunto de componentes de administración de sistemas más estandarizado. El SM-CLP de SMWG es un subcomponente de los esfuerzos generales de SMASH realizados por el DMTF.

El SM-CLP ofrece un subconjunto de funciones de la interfaz de línea de comandos de RACADM local, pero con una ruta de acceso distinta. SM-CLP se ejecuta dentro del iDRAC6, mientras que RACADM se ejecuta en el servidor administrado. Asimismo, RACADM es una interfaz patentada de Dell; SM-CLP es una interfaz estándar de la industria.

NOTA: El sitio web **delltechcenter.com** del Dell Enterprise Technology Center tiene disponible información sobre los perfiles de Dell y los MOF y toda la información del DMTF se encuentra disponible en el sitio web **dmtf.org/standards/profiles/**. Además, las extensiones de Dell están disponibles en **delltechcenter.com/page/DCIM+-+Dell+CIM+Extensions**.

Administración del sistema por medio de SM-CLP

El SM-CLP del iDRAC6 permite administrar las siguientes funciones de sistema desde una línea de comandos:

- Administración de la alimentación de servidor: enciende, apaga o reinicia el sistema
- Administración de registro de sucesos del sistema (SEL): muestra o borra las anotaciones del registro de sucesos del sistema
- Administración de cuentas de usuario del iDRAC6
- Configuración de Active Directory
- Configuración de la LAN del iDRAC6
- Generación de solicitudes de firma de certificados (CSR) de SSL
- Configuración de los medios virtuales

Compatibilidad con SM-CLP de iDRAC6

SM-CLP se aloja en el firmware del iDRAC6 y es compatible con conexiones Telnet y SSH. La interfaz de SM-CLP del iDRAC6 está basada en la versión 1.0 de la especificación SM-CLP proporcionada por DMTF.

Las siguientes secciones proporcionan una descripción de la función SM-CLP que se aloja en el iDRAC6.

NOTA: Si estableció una sesión SM–CLP a través de Telnet/SSH y la sesión no se cierra correctamente debido a una desconexión de la red, es posible que se muestre un mensaje de error para indicar que alcanzó la cantidad máxima de conexiones. Para resolver este problema, termine la sesión SM–CLP en la interfaz gráfica del usuario de web en **Sistema**→ **Configuración de iDRAC**→ **Red/Seguridad**→ **Sesiones** antes de intentar establecer una nueva sesión.

NOTA: El iDRAC6 admite un máximo de 4 sesiones de Telnet y 4 sesiones de SSH de forma simultánea. No obstante, sólo *una* de las 8 sesiones posibles puede utilizar SM-CLP. Es decir, el iDRAC6 admite solamente una sesión SM-CLP por vez.

Cómo iniciar una sesión SM–CLP

- Conéctese al iDRAC6 a través de SSH/Telnet para ir a la interfaz de línea de comandos (consola).
- Introduzca “smclp” en la solicitud del símbolo de dólar para iniciar la consola SM–CLP.

Sintaxis:

```
telnet <dirección_IP_iDRAC6>
```

```
$ (se muestra la solicitud de la interfaz de línea
de comandos)
```

```
$smclp (en la solicitud de la interfaz de línea de
comandos, escriba smclp)
```

Funciones de SM-CLP

La especificación SM-CLP proporciona un conjunto común de verbos estándares de SM-CLP que se pueden utilizar para la administración simple de sistemas por medio de la CLI.

El SM-CLP promueve el concepto de verbos y destinos para ofrecer capacidades de configuración de sistemas por medio de la CLI. El verbo indica la operación a realizar, mientras que el destino es la entidad (u objeto) en la que se ejecuta dicha operación.

A continuación se presenta la sintaxis de la línea de comandos de SM-CLP:

```
<verb> [<options>] [<target>] [<properties>]
```

La Tabla 15-1 muestra una lista de verbos compatibles con la CLI del iDRAC6, la sintaxis de cada comando y una lista de opciones compatibles con el verbo.

Tabla 15-1. Verbos compatibles con la CLI de SM-CLP

Verbo	Descripción	Opciones
cd	Se desplaza por el espacio de direcciones de sistema administrado por medio del shell. Sintaxis: `cd [opciones] [destino]`	–default, –examine, –help, –output, –version
delete	Elimina un objeto. Sintaxis: `delete [opciones] destino`	–examine, –help, –output, –version
exit	Cierra la sesión de shell de SM-CLP. Sintaxis: `exit [opciones]`	–help, –output, –version

Tabla 15-1. Verbos compatibles con la CLI de SM-CLP *(continuación)*

Verbo	Descripción	Opciones
help	Muestra la ayuda de los comandos de SM-CLP. `help`	-examine, -help, -output, -version
reset	Restablece el destino. Sintaxis: `reset [opciones] [destino]`	–examine, –help, –output, –version
set	Establece las propiedades de un destino Sintaxis: `set [opciones] [destino] <nombre de propiedad>=<valor>`	–examine, –help, –output, –version
show	Muestra las propiedades, verbos y subdestinos del destino. Sintaxis: `show [opciones] [destino] <nombre de propiedad>=<valor>`	-all, -default, –display, –examine, –help, –level, –output, –version
start	Inicia un destino. Sintaxis: `start [opciones] [destino]`	–examine, –force, –help, –output, –version
stop	Desactiva un destino. Sintaxis: `stop [opciones] [destino]`	–examine, –force, –help, –output, –version, –wait
version	Muestra los atributos de versión de un destino. Sintaxis: `version [opciones]`	–examine, –help, –output, –version

Tabla 15-2 describe las opciones de SM-CLP. Algunas opciones están en forma abreviada, según se muestra en la tabla.

Tabla 15-2. Opciones admitidas por SM-CLP

Opción de SM-CLP	Descripción
-all, -a	Indica al verbo que va a realizar todas las funciones posibles.
-destination	Especifica la ubicación para almacenar una imagen en el comando dump. Sintaxis: –destination <URI>
-display, -d	Filtra la salida generada por el comando. Sintaxis: `-display <properties | targets | verbs> [, <properties | targets | verbs>]*`
-examine, -x	Indica al procesador de comandos que va a validar la sintaxis del comando sin ejecutarlo.
-force, -f	Si no se logra un apagado ordenado, utilice esta opción para forzar el apagado del sistema de destino. Sintaxis: `stop -force <target>`
-help, -h	Muestra la ayuda del verbo.
-level, -l	Indica al verbo que opere en destinos de niveles adicionales debajo del destino especificado. Sintaxis: `-level <n | all>`

-output, -o	Especifica el formato de la salida.
	Sintaxis:
	`-output format=<text | clpcsv | keyword | clpxml>`
	o
	`-o format=<text | clpcsv | keyword | clpxml>`

-version, -v	Muestra el número de versión de SM–CLP.

Navegación en el espacio de direcciones de MAP

NOTA: La barra diagonal (/) y la barra diagonal invertida (\) pueden intercambiarse en las rutas de acceso de direcciones en SM-CLP. Sin embargo, una barra diagonal invertida al final de una línea de comandos hace que el comando continúe en la línea siguiente y se ignora cuando el comando se ejecuta.

Los objetos que pueden ser administrados con SM-CLP se representan con destinos organizados en un espacio jerárquico denominado espacio de direcciones de punto de acceso de administrabilidad (MAP). La ruta de acceso de la dirección especifica la ruta de acceso desde la raíz del espacio de direcciones hacia un objeto en el espacio de direcciones.

El destino raíz se representa con una barra diagonal (/) o una barra diagonal invertida (\). Es el punto de partida predeterminado cuando se inicia sesión en el iDRAC6. Desplácese a la raíz con el verbo `cd`.

Por ejemplo, para navegar a la tercera anotación en el Registro de sucesos del sistema (SEL), introduzca el siguiente comando:

```
->cd /admin1/system1/logs1/log1/record3
```

Introduzca el verbo `cd` sin destino para encontrar la ubicación actual en el espacio de direcciones. Las abreviaturas `..` y `.` funcionan de la misma forma como funcionan en Windows y Linux: `..` se refiere al nivel superior inmediato y `.` se refiere al nivel actual.

Destinos

Para consultar una lista de destinos disponibles a través de SM-CLP, consulte el documento de asignación de SM–CLP disponible en Dell Enterprise Technology Center en **delltechcenter.com**.

Uso del verbo show

Para conocer más acerca de un destino, utilice el verbo `show`. Este verbo muestra las propiedades del destino, los subdestinos, asociaciones y una lista de verbos de SM-CLP que se permiten en la ubicación.

Uso de la opción -display

La opción **show -display** permite limitar la salida del comando de manera que muestre una o más propiedades, destinos, asociaciones y verbos. Por ejemplo, para mostrar sólo las propiedades y destinos en la ubicación actual, utilice el siguiente comando:

```
show -display properties,targets
```

Para mostrar sólo ciertas propiedades, indíquelas según se muestra en el siguiente comando:

```
show –d properties=(userid,name)
/admin1/system1/sp1/oemdcim_mfaaccount1
```

Si sólo desea mostrar una propiedad, puede omitir los paréntesis.

Uso de la opción -level

La opción **show -level** ejecuta **show** en niveles adicionales debajo del destino especificado. Para consultar todos los destinos y las propiedades en el espacio de direcciones, utilice la opción **-l all**:

Uso de la opción -output

La opción **-output** especifica uno de cuatro formatos para la salida de los verbos de SM-CLP: **text**, **clpcsv**, **keyword** y **clpxml**.

El formato predeterminado es **text** y es el mensaje de salida más legible. El formato **clpcsv** es un formato de valores separados con comas que es apto para cargar un programa de hoja de cálculo. El formato **keyword** (palabra clave) muestra la información en forma de lista de pares palabra_clave=valor, un par por cada línea. El formato **clpxml** es un documento XML que contiene el elemento XML **response**. El Grupo de trabajo de administración distribuida (DMTF) creó especificaciones para los formatos **clpcsv** y **clpxml** que se encuentran en su sitio web en **dmtf.org**.

El siguiente ejemplo muestra cómo incluir el contenido del registro de sucesos del sistema en el mensaje de salida de XML:

```
show -l all -output format=clpxml
/admin1/system1/logs1/log1
```

Ejemplos de SM-CLP del iDRAC6

Las siguientes subsecciones ofrecen ejemplos sobre cómo iniciar sesión en el iDRAC6 mediante la interfaz SSH e iniciar una sesión SM-CLP para realizar las siguientes operaciones:

- Administración de la alimentación del servidor
- Administración de SEL
- Navegación en el mapa de destino
- Mostrar las propiedades del sistema

Administración de la alimentación del servidor

La Tabla 15-3 contiene ejemplos de cómo utilizar SM-CLP para realizar operaciones de administración de la alimentación del servidor en un servidor administrado.

Escriba "`smclp`" para iniciar la consola SM-CLP.

Tabla 15-3. Operaciones de administración de la alimentación del servidor

Operación	Sintaxis

Inicio de sesión en el iDRAC6 por medio de la interfaz SSH	`>ssh 192.168.0.120`
	`>login: root`
	`>password:`
	Escriba "`smclp`" para iniciar la consola SM–CLP.

Apagar el servidor	`->stop /admin1/system1` `system1 successfully stopped`
Encender el servidor a partir de un estado apagado	`->start /admin1/system1` `system1 successfully started`
Reiniciar el servidor	`->reset /admin1/system1` `RESET successful for system 1`

Administración de SEL

La Tabla 15-4 contiene ejemplos de cómo utilizar SM-CLP para ejecutar operaciones relacionadas con SEL en el sistema administrado.

Navegación en MAP del destino

La Tabla 15-5 muestra ejemplos de cómo utilizar el verbo **cd** para navegar en MAP. En todos los ejemplos, se supone que el destino inicial predeterminado es /.

Tabla 15-4. Operaciones de administración del registro de sucesos del sistema

Operación	Sintaxis

Ver el SEL	`->show -d targets,properties,verbs /admin1/system1/logs1/log1`
	
	Podría informar lo siguiente:
	`Destinos:`
	`record1/`
	`record2/...`
	
	`Propiedades:`
	`OverwritePolicy=7`
	`LogState=4`
	`CurrentNumberOfRecords=60`
	`MaxNumberOfRecords=512`
	`ElementName=Record Log 1`
	`HealthState=5`
	`EnabledState=2`
	`RequestedState=12`
	`EnabledDefault=2`
	`TransitioningToState=12`
	`InstanceID=DCIM: SEL Log`
	`OperationalStatus={2}`
	
	`Verbos:`
	`show`
	`exit`
	`version`
	`cd`
	`help`

Tabla 15-4. Operaciones de administración del registro de sucesos del sistema *(continuación)*

Operación	Sintaxis
Ver el registro de SEL	`->show /admin1/system1/logs1/log1/record4` Podría informar lo siguiente: `ufip=/admin1/system1/logs1/log1/record4` `Associations:LogManagesRecord= >/admin1/system1/logs1/log1` `Propiedades:` `RecordData=*0.0.65*4 2*1245152621*65 65*4*31*0*true*111*1*255*255* RecordFormat= *IPMI_SensorNumber.IPMI_OwnerLUN.IPMI_OwnerID*I PMI_RecordID*IPMIRecordType*IPMI_TimeStamp*IPMI _GeneratorID*IPMI_EvMRev*IPMI_SensorType*IPMI_S ensorNumber*IPMI_AssertionEvent*IPMI_EventType* IPMI_EventData1*IPMI_EventData2*IPMI_EventData3 *IANA*`  `Description=:0:Assert:OEM specific`  `ElementName=DCIM System Event Log Entry (Anotación del registro de sucesos del sistema DCIM)`  `InstanceID=DCIM:SEL LOG:4`  `LogInstanceID=idrac:Unknown:Unknown SEL Log`  `LogName=DCIM System Event Log Entry`  `RecordID=DCIM:SEL LOG:4`  `CreationTimeStamp=20090616114341.000000+000`

Tabla 15-4. Operaciones de administración del registro de sucesos del sistema *(continuación)*

Operación	Sintaxis
	Verbos: show exit version cd help delete
Borrar el SEL	->delete /admin1/system1/logs1/log1/record* Informa: Records deleted successfully (Registros eliminados correctamente).

Tabla 15-5. Operaciones de navegación del mapa de destino

Operación	Sintaxis
Navegar hacia el sistema destino y reiniciar	->cd admin1/system1 ->reset **NOTA:** El destino predeterminado actual es /.
Navegar hacia el registro de sucesos del sistema (SEL) de destino y mostrar las anotaciones del registro	->cd admin1 ->cd system1 ->cd logs1 ->cd log1 ->show es igual a ->cd admin1/system1/logs1/log1 ->show
Mostrar el destino actual	->cd .
Subir un nivel	->cd ..
Salir del shell	->exit

16

Uso de la interfaz WS-MAN

Servicios web para administración (WS–MAN) es un protocolo basado en el protocolo simple de acceso a objetos (SOAP), utilizado en la administración de sistemas. WS–MAN proporciona un protocolo con capacidad interoperativa para que los dispositivos puedan compartir e intercambiar datos a través de redes. El iDRAC6 utiliza WS–MAN para transmitir información de administración basada en el modelo común de información (CIM) del grupo de trabajo de administración distribuida (DMTF); la información del CIM define la semántica y los tipos de información que pueden manipularse en un sistema administrado. Las interfaces incorporadas por Dell para la administración de plataformas de servidores están organizadas en perfiles, en los que cada perfil define las interfaces específicas para cada dominio de administración o área de funcionalidad en particular. Además, Dell ha definido diversas extensiones de modelo y perfil que ofrecen interfaces para otras capacidades.

Los datos que se encuentran disponibles a través de WS-MAN son provistos por la interfaz de instrumentación del iDRAC6 asignada a los perfiles de DMTF y de extensión de Dell.

Funciones de WS-Management

La especificación WS–Management promueve la interoperabilidad entre aplicaciones de administración y recursos administrados. Al identificar un conjunto principal de especificaciones de servicios web y requisitos de uso para exhibir un conjunto común de operaciones centrales para la administración de todos los sistemas, WS–Management es capaz de hacer lo siguiente:

- DETECTAR la presencia de recursos administrados y trasladarse entre ellos
- OBTENER, ESTABLECER, CREAR Y ELIMINAR recursos individuales de administración, como configuraciones y valores dinámicos
- ENUMERAR el contenido de contenedores y recopilaciones, como registros y tablas de gran tamaño
- EJECUTAR métodos específicos de administración con parámetros de entrada y salida con establecimiento inflexible de tipos

Perfiles CIM admitidos

Tabla 16-1. Perfiles CIM admitidos

DMTF estándar
1 Servidor básico Define las clases de CIM para representar al servidor host.
2 Métricas básicas Define las clases de CIM para ofrecer la capacidad de modelar y controlar las métricas capturadas para elementos administrados.
3 Procesador de servicio Define las clases de CIM para modelar procesadores de servicio.
4 Redirección de USB Define las clases de CIM para describir información acerca de las redirecciones de USB. Para dispositivos de teclado, vídeo y mouse, este perfil debe usarse si los dispositivos se van a administrar como dispositivos USB.
5 Propiedad física Define las clases de CIM para representar el aspecto físico de los elementos administrados. El iDRAC6 usa este perfil para representar la información de FRU del servidor host y de sus componentes, además de la tipología física.
6 Admin de dominios SM-CLP Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del CLP.
7 Administración del estado de la alimentación Define las clases de CIM para las operaciones de control de alimentación. El iDRAC6 usa este perfil para las operaciones de control de alimentación del servidor host.
8 Servicio CLP Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del CLP.
9 Interfaz IP Define las clases de CIM para representar la interfaz IP de un sistema administrado.
10 Cliente DHCP Define las clases de CIM para representar un cliente DHCP y sus funciones y configuración asociadas.

Tabla 16-1. Perfiles CIM admitidos *(continuación)*

DMTF estándar
11 Cliente DNS Define las clases de CIM para representar un cliente DNS en un sistema administrado.
12 Registro Define las clases de CIM para representar distintos tipos de registros. El iDRAC6 usa este perfil para representar el registro de sucesos del sistema (SEL) y el registro RAC del iDRAC6.
13 Autorización basada en funciones Define las clases de CIM para representar funciones. El iDRAC6 usa este perfil para configurar privilegios de la cuenta iDRAC6.
14 Recopilación SMASH Define las clases de CIM para representar la configuración del CLP. El iDRAC6 usa este perfil para su propia implementación del CLP.
15 Registro de perfiles Define las clases de CIM para anunciar las implementaciones de perfil. El iDRAC6 usa este perfil para anunciar sus propios perfiles implementados, como se describe en esta tabla.
16 Administración de identidad simple Define las clases de CIM para representar identidades. El iDRAC6 usa este perfil para la configuración de cuentas iDRAC6.
17 Puerto Ethernet Define las clases de CIM para representar un puerto Ethernet, su controlador asociado y las interfaces Ethernet en un sistema administrado. Las asociaciones con los aspectos físicos del puerto y la información de la versión de la implementación del perfil se modelan en este perfil.
18 Sensor Define las clases de CIM utilizadas para describir los sensores en un sistema administrado. También define las clases de asociaciones que describen la relación de los sensores con los dispositivos supervisados.

Tabla 16-1. Perfiles CIM admitidos *(continuación)*

Extensiones de Dell
1 Cliente Active Directory Define las clases de extensiones de CIM y Dell para configurar el cliente iDRAC6 Active Directory y los privilegios locales para grupos de Active Directory.
2 Medios virtuales Define las clases de extensiones de CIM y Dell para configurar los medios virtuales del iDRAC6. Extiende el perfil de *redirección de USB*.
3 Implementación de sistema operativo Define las clases de extensión de CIM y Dell para representar la configuración de las funciones de implementación de sistema operativo. Amplía la función de administración de hacer referencia a los perfiles al sumar la compatibilidad con actividades de implementación de sistema operativo manipulando las funciones de ese tipo de implementación que ofrece el procesador de servicio.
4 Inventario de software Define las extensiones de Dell y CIM para representar las versiones actualmente instaladas del BIOS, firmware de componentes, diagnósticos, Unified Server Configurator y de los paquetes Driver Pack de controladores. Asimismo, proporciona una representación de las versiones de las imágenes de actualización del BIOS y el firmware que se encuentran disponibles en Lifecycle Controller para reversión y reinstalación.
5 Actualización de software Define las extensiones de CIM y Dell para la representación de los métodos y la clase de servicio para actualizar el BIOS, diagnósticos, paquete de controladores y firmware de componentes y Lifecycle Controller. Los métodos de actualización admiten la actualización desde ubicaciones de recursos compartidos de red CIFS, NFS, FTP y HTTP, así como desde las imágenes de actualización situadas en Lifecycle Controller. Las solicitudes de actualización se emiten como trabajos y pueden programarse de inmediato o posteriormente con varias opciones de tipos de acciones de reinicio para aplicar las actualizaciones.
6 Control de trabajos Define las extensiones de CIM y Dell para la administración de los trabajos generados por las solicitudes de actualización. Los trabajos pueden crearse, eliminarse, modificarse y agregarse a colas de espera de trabajos para establecer una secuencia y ejecutar múltiples actualizaciones en un solo reinicio.

Tabla 16-1. Perfiles CIM admitidos *(continuación)*

Extensiones de Dell
7 Administración de LC Define las extensiones de CIM y Dell que permiten obtener y definir los atributos para administrar las funciones de descubrimiento automático y reemplazo de piezas del controlador Lifecycle Controller.
8 Almacenamiento persistente Define las clases de extensiones de CIM y Dell para administrar las particiones de las unidades flash virtuales de las plataformas Dell.
9 NIC simple Define las clases de extensiones de CIM y Dell para representar la configuración de los controladores de red de NIC.
10 BIOS y la administración del inicio Define las clases de extensiones de CIM y Dell que representan los atributos del BIOS de Dell para configurar la secuencia de inicio del host.
11 RAID simple Define las clases de extensiones de CIM y Dell que representan la configuración del almacenamiento RAID del host.
12 Tarjeta iDRAC Define las clases de extensiones de CIM y Dell para representar la información de inventario del iDRAC6.
13 Memoria Define las clases de extensiones de CIM y Dell para representar la información de inventario del DIMM del host.
14 CPU Define las clases de extensiones de CIM y Dell para representar la información de inventario del CPU del host.
15 Información del sistema Define las clases de extensiones de CIM y Dell para representar la información de inventario de la plataforma del host.
16 Dispositivo PCI Define las clases de extensiones de CIM y Dell para representar la información de inventario del PCI del host.
17 Vídeo Define las clases de extensiones de CIM y Dell para representar la información de inventario de la tarjeta de vídeo del host.

La implementación de WS-MAN del iDRAC6 utiliza SSL en el puerto 443 para garantizar la seguridad de transporte y admite autenticación básica. Las interfaces de servicios web se pueden utilizar aprovechando la infraestructura cliente, como la CLI de WinRM y Powershell de Windows, utilidades de código fuente abierto como WSMANCLI y entornos de programación de aplicaciones como Microsoft .NET.

Encontrará guías de implementación adicionales, documentos técnicos, perfiles, MOF y códigos en el Enterprise Technology Center de Dell en **delltechcenter.com**. Para obtener más información, consulte también:

- Sitio web de DMTF: **dmtf.org/standards/profiles/**
- Notas de publicación o archivo léame de WS–MAN.

17

Implementación del sistema operativo por medio de iVMCLI

La utilidad de interfaz de línea de comandos de soportes virtuales integrada (iVMCLI) es una interfaz de línea de comandos que ofrece las funciones de soportes virtuales desde la estación de administración al iDRAC6 en el sistema remoto. Por medio de la iVMCLI y los métodos con secuencias de comandos, es posible implementar el sistema operativo en varios sistemas remotos en la red.

Esta sección contiene información acerca de cómo integrar la utilidad iVMCLI en su red de la empresa.

Antes de comenzar

Antes de usar la utilidad iVMCLI, asegúrese de que los sistemas remotos de destino y la red de la empresa cumplan con los requisitos que se enumeran en las siguientes secciones.

Requisitos del sistema remoto

- El iDRAC6 se configura en cada sistema remoto.

Requisitos de red

Un recurso compartido de red debe tener los siguientes componentes:

- Los archivos del sistema operativo
- Los archivos controladores requeridos
- Los archivos de imagen de inicio del sistema operativo

  El archivo de imagen debe ser un CD de sistema operativo o una imagen ISO de CD/DVD, con un formato de inicio estándar de la industria.

Creación de un archivo de imagen de inicio

Antes de implementar el archivo de imagen en los sistemas remotos, compruebe que un sistema admitido pueda iniciar a partir del archivo. Para probar el archivo de imagen, transfiéralo a un sistema de prueba por medio de la interfaz web de usuario del iDRAC6 y reinicie el sistema.

Las siguientes secciones contienen información específica para la creación de archivos de imagen para sistemas Linux y Windows.

Creación de un archivo de imagen para sistemas Linux

Use la utilidad de duplicador de datos (dd) para crear un archivo de imagen de inicio para el sistema Linux.

Para ejecutar la utilidad, abra una ventana de símbolo del sistema y escriba lo siguiente:

```
dd if=<input-device> of=<output-file>
```

Por ejemplo,

```
dd if=/dev/sdc0 of=mycd.img
```

Creación de un archivo de imagen para sistemas Windows

Al momento de elegir una utilidad de replicador de datos para crear archivos de imagen de Windows, seleccione una utilidad que copie el archivo de imagen y los sectores de inicio de CD/DVD.

Preparación para la implementación

Configuración de sistemas remotos

1. Cree un recurso compartido de red al que pueda acceder desde la estación de administración.
2. Copie los archivos del sistema operativo en el recurso compartido de red.
3. Si tiene un archivo de imagen de inicio preconfigurado para implementar el sistema operativo en los sistemas remotos, omita este paso.

   Si no tiene un archivo de imagen de inicio preconfigurado para implementación, prepárelo. Incluya los programas o secuencias de comandos que se van a utilizar en los procedimientos de implementación del sistema operativo.

Por ejemplo, para implementar un sistema operativo Microsoft Windows, el archivo de imagen puede incluir programas similares a los métodos de implementación que utiliza Microsoft Systems Management Server (SMS).

Al momento de crear el archivo de imagen, haga lo siguiente:

- Siga los procedimientos estándares de instalación basada en red.
- Marque la imagen de implementación como "de sólo lectura" para garantizar que cada sistema de destino se inicie y ejecute el mismo procedimiento de implementación.

4 Realice uno de los procedimientos siguientes:

- Integre **IPMItool** y la interfaz de línea de comandos de soportes virtuales (iVMCLI) en la aplicación existente de implementación del sistema operativo. Use la secuencia de comandos de ejemplo **ivmdeploy** como guía para usar la utilidad.
- Utilice la secuencia de comandos **ivmdeploy** existente para implementar el sistema operativo.

NOTA: ivmdeploy usa internamente iVMCLI y ipmitool. Para usar esta herramienta debe contar con privilegios para *IPMI en la LAN*. Asimismo, los soportes virtuales deben estar en estado conectado cuando utilice la secuencia de comandos ivmdeploy.

Implementación del sistema operativo

Use la utilidad iVMCLI y la secuencia de comandos **ivmdeploy** que se incluye con la utilidad para implementar el sistema operativo en los sistemas remotos.

Antes de comenzar, repase la secuencia de comandos **ivmdeploy** de ejemplo que se incluye con la utilidad iVMCLI. La secuencia de comandos muestra los pasos detallados que se necesitan para implementar el sistema operativo en los sistemas remotos de la red.

El siguiente procedimiento ofrece una descripción de alto nivel para implementar el sistema operativo en los sistemas remotos de destino.

1 Haga una lista de las direcciones IP de iDRAC6 de los sistemas remotos que serán implementados en el archivo de texto **ip.txt**, una dirección IP por línea.

2. Inserte un CD o DVD de inicio de sistema operativo en la unidad correspondiente del cliente.
3. Ejecute **ivmdeploy** en la línea de comandos.

Para ejecutar la secuencia de comandos ivmdeploy, introduzca el siguiente comando en el símbolo del sistema:

```
ivmdeploy -r ip.txt -u <idrac-user> -p <idrac-passwd>
-c {<imagen_iso9660> | <path>}
```

donde:

- <*usuario_del_idrac*> es el nombre del usuario del iDRAC6, por ejemplo, **root**
- <*contraseña_del_idrac*> es la contraseña del usuario del iDRAC6, por ejemplo, **calvin**
- <*imagen_iso9660*> es la ruta de acceso de la imagen ISO9660 del CD o DVD de instalación del sistema operativo
- <*ruta_de_acceso*> es la ruta de acceso del dispositivo que contiene el CD o DVD de instalación del sistema operativo

La secuencia de comandos **ivmdeploy** pasa las opciones de línea de comandos a la utilidad **iVMCLI**. Ver "Opciones de la línea de comandos" en la página 356 para obtener detalles sobre estas opciones. La secuencia de comandos procesa la opción **-r** de manera un poco distinta a la opción **iVMCLI -r**. Si el argumento de la opción **-r** es el nombre de un archivo existente, la secuencia de comandos leerá las direcciones IP de iDRAC6 del archivo especificado y ejecutará la utilidad **iVMCLI** una vez por cada línea. Si el argumento de la opción **-r** no es un nombre de archivo, debe ser entonces la dirección de un solo iDRAC6. En este caso, la opción **-r** funciona como se describe en la utilidad **iVMCLI**.

La secuencia de comandos ivmdeploy admite únicamente instalaciones a partir de un CD/DVD o de una imagen ISO9660 de CD/DVD. Si necesita instalar a partir de un disco flexible o de una imagen de disco flexible, puede modificar la secuencia de comandos para usar la opción **iVMCLI -f**.

Uso de la utilidad de interfaz de línea de comandos de los soportes virtuales

La utilidad de interfaz de línea de comandos de soportes virtuales (iVMCLI) se puede usar con secuencias de comandos y suministra las funciones de soportes virtuales de la estación de administración al iDRAC6.

La utilidad iVMCLI ofrece las siguientes funciones:

NOTA: Al hacer virtuales los archivos de imagen de sólo lectura, es posible que varias sesiones compartan el mismo medio de imagen. Al hacer virtuales las unidades físicas, sólo una sesión a la vez puede acceder a una unidad física determinada.

- Dispositivos de medios extraíbles o archivos de imagen que son coherentes con los complementos de medios virtuales
- Finalización automática cuando está activada la opción de inicio único del firmware del iDRAC6
- Comunicaciones seguras con el iDRAC6 por medio de la capa de sockets seguros (SSL)

Antes de que ejecutar la utilidad, compruebe que cuenta con privilegios de usuario de soportes virtuales en el iDRAC6.

PRECAUCIÓN: Se recomienda usar la opción '-i' de marcador interactivo al iniciar la utilidad de línea de comandos iVMCLI. Esto garantiza mayor seguridad al mantener en privado el nombre de usuario y la contraseña, ya que en muchos sistemas operativos Windows y Linux el nombre de usuario y la contraseña son visibles en formato de texto simple cuando los procesos son examinados por otros usuarios.

Si el sistema operativo admite los privilegios de administrador o una pertenencia a grupos o privilegio específico del sistema operativo, también deberá tener privilegios de administrador para poder ejecutar el comando iVMCLI.

El administrador del sistema cliente controla los privilegios y grupos de usuarios, por consiguiente, controla cuáles usuarios pueden ejecutar la utilidad.

Para sistemas Windows, se deben tener privilegios de usuario avanzado para poder ejecutar la utilidad iVMCLI.

En los sistemas Linux, se puede acceder a la utilidad iVMCLI sin tener privilegios de administrador por medio del comando **sudo**. Este comando proporciona un medio centralizado para dar acceso sin privilegio de administrador y registra todos los comandos de usuario.

Para agregar o editar usuarios en el grupo iVMCLI, el administrador usa el comando **visudo**. Los usuarios sin privilegios de administrador pueden agregar el comando **sudo** como prefijo a la línea de comandos de iVMCLI (o a la secuencia de comandos de iVMCLI) a fin de obtener acceso al iDRAC6 en el sistema remoto y ejecutar la utilidad.

Instalación de la utilidad iVMCLI

La utilidad iVMCLI se encuentra en el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) que se incluye en el paquete de software Dell OpenManage System Management. Para instalar la utilidad, inserte el DVD en el sistema y siga las instrucciones que aparecen en la pantalla.

El DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) contiene los productos de software de administración de sistemas más recientes, incluso los diagnósticos, la administración de almacenamiento, el servicio de acceso remoto y la utilidad RACADM. Este DVD también contiene archivos léame con la más reciente información de producto del software de administración de sistemas.

Además, el DVD *Dell Systems Management Tools and Documentation* (Documentación y herramientas de Dell Systems Management) también incluye **vmdeploy**: una secuencia de comandos de ejemplo que ilustra el uso de las utilidades iVMCLI y RACADM para implementar software en varios sistemas remotos.

NOTA: La secuencia de comandos **ivmdeploy** depende de otros archivos que están presentes en el directorio de la misma cuando se instala. Si desea usar la secuencia de comandos desde otro directorio, copie todos los archivos con ella.

Opciones de la línea de comandos

La interfaz iVMCLI es idéntica en los sistemas Windows y Linux. La utilidad usa opciones que son congruentes con las opciones de la utilidad RACADM. Por ejemplo, una opción para especificar la dirección IP de iDRAC6 requiere la misma sintaxis tanto en la utilidad RACADM como en la utilidad iVMCLI.

El formato del comando de iVMCLI es como se indica a continuación:

`iVMCLI [parameter] [operating_system_shell_options]`

En la sintaxis de la línea de comandos se distingue entre mayúsculas y minúsculas. Ver "Parámetros de iVMCLI" en la página 357 para obtener más información.

Si el sistema remoto acepta los comandos y el iDRAC6 autoriza la conexión, el comando seguirá ejecutándose hasta que se presente cualquiera de los siguientes casos:

- La conexión de iVMCLI termina por algún motivo.
- El proceso se termina manualmente por medio de un control de sistema operativo. Por ejemplo, en Windows, se puede usar el Administrador de tareas para terminar el proceso.

NOTA: Cuando se usa el comando iVMCLI, si los valores de los parámetros tienen espacios entre las palabras, se debe encerrar entre comillas el valor completo del parámetro. Por ejemplo, tomemos el comando para adjuntar una imagen de DVD de su sistema al sistema operativo del servidor:
F:\idrac>ivmcli -r 10.35.155.117 -u root -p calvin -c c:\documents and settings\usuario\mis documentos\work\devel\omsa\img_hdd1.iso

donde, -c es uno de los parámetros y **c:\documents and settings\user\my documents\work\devel\omsa\img_hdd1.iso** es el valor del parámetro que contiene espacios para "documents and settings" y "my documents". Por lo tanto se usan comillas para encerrar la ruta de acceso completa del archivo de imagen. Sin las comillas, el comando fallará. Lo siguiente tampoco es válido:

C:\"documents and settings"\.....

Parámetros de iVMCLI

Dirección IP del iDRAC6

`-r <dirección_IP_del_iDRAC>[:<puerto_SSL_del_iDRAC>]`

Este parámetro proporciona la dirección IP del iDRAC6 y el puerto SSL, con los que la utilidad debe establecer una conexión de soportes virtuales con el iDRAC6 de destino. Si introduce un nombre de DDNS o una dirección IP no válida, aparecerá un mensaje de error y el comando terminará.

<*dirección_IP_de_iDRAC6*> es una dirección IP válida y única, o bien un nombre de sistema dinámico de nombres de dominio (DDNS) de iDRAC6 (si se admite). Si se omite <*Puerto_SSL_de_iDRAC*>, se utilizará el puerto 443 (el puerto predeterminado). El puerto SSL opcional no es necesario a menos que se haya cambiado el puerto SSL predeterminado del iDRAC6.

Nombre de usuario del iDRAC6

`-u <iDRAC-user-name>`

Este parámetro proporciona el nombre de usuario del iDRAC6 que ejecutará los soportes virtuales.

El <*nombre_de_usuario_del_iDRAC*> debe tener los atributos siguientes:

- Nombre de usuario válido
- Permiso de usuario de medios virtuales del iDRAC6

Si la autentificación de iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Contraseña de usuario del iDRAC6

`-p <iDRAC-user-password>`

Este parámetro proporciona la contraseña para el usuario del iDRAC6 especificado.

Si la autentificación de iDRAC6 falla, aparecerá un mensaje de error y se finalizará el comando.

Archivo de imagen o dispositivo de disco/disco flexible

`-f {<device-name> | <image-file>}`

donde <*nombre_de_dispositivo*> es una letra de unidad válida (para sistemas Windows) o un nombre de archivo de dispositivo válido, incluyendo el número de partición del sistema de archivos montable, de ser aplicable (para sistemas Linux); y <*archivo_de_imagen*> es el nombre y la ruta de acceso de un archivo de imagen válido.

Este parámetro especifica el dispositivo o archivo que va a proporcionar el medio virtual de disco o disco flexible.

Por ejemplo, un archivo de imagen se especifica como:

`-f c:\temp\myfloppy.img` (sistema Windows)

`-f /tmp/myfloppy.img` (sistema Linux)

Si el archivo no está protegido contra escritura, es posible que los medios virtuales escriban en el archivo de imagen. Configure el sistema operativo para proteger contra escritura una imagen de disco flexible que no desea que se sobrescriba.

Por ejemplo, un dispositivo se especifica como:

`-f a:\` (sistema Windows)

`-f /dev/sdb4 # 4th partition on device /dev/sdb` (sistema Linux)

Si el dispositivo tiene capacidad de protección contra escritura, utilice esta capacidad para garantizar que los medios virtuales no escribirán en el medio.

Omita este parámetro de la línea de comandos si no va a virtualizar discos flexibles. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Archivo de imagen o dispositivo de CD/DVD

`-c {<device-name> | <image-file>}`

donde <*device-name*> es una letra de unidad de CD/DVD válida (sistemas Windows) o un nombre de archivo de dispositivo CD/DVD válido (sistemas Linux) y <*image-file*> es el nombre y la ruta de acceso de un archivo de imagen ISO-9660 válido.

Este parámetro especifica el dispositivo o archivo que proporcionará el soporte virtual de CD/DVD-ROM:

Por ejemplo, un archivo de imagen se especifica como:

`-c c:\temp\mydvd.img` (sistemas Windows)

`-c /tmp/mydvd.img` (sistemas Linux)

Por ejemplo, un dispositivo se especifica como:

`-c d:\` (sistemas Windows)

`-c /dev/cdrom` (sistemas Linux)

Omita este parámetro de la línea de comandos si no va a virtualizar soportes multimedia de CD/DVD. Si se detecta un valor no válido, aparecerá un mensaje de error y el comando terminará.

Especifique al menos un tipo de medio (disco flexible o unidad de CD/DVD) con el comando, salvo que sólo se tengan opciones de interruptor. De lo contrario, aparecerá un mensaje de error y el comando terminará y producirá un error.

Validación del certificado de CA de raíz

`-s`

Este parámetro se usa para indicar si el certificado de CA del iDRAC es válido o no. Si el certificado no es válido, finaliza la sesión de la iVMCLI y se muestra un mensaje de error que indica que el certificado no es válido. Si el certificado es válido, se establece la sesión de la iVMCLI.

Mostrar la versión

`-v`

Este parámetro se usa para mostrar la versión de la utilidad iVMCLI. Si no se proporcionan otras opciones además de interruptores, el comando terminará sin mensajes de error.

Mostrar la ayuda

`-h`

Este parámetro muestra un resumen de los parámetros de la utilidad iVMCLI. Si no se proporcionan otras opciones además de conmutadores, el comando termina sin errores.

Consulta del manual

`-m`

Este parámetro muestra una "página de manual" detallada de la utilidad iVMCLI, incluidas las descripciones de todas las opciones posibles.

Datos cifrados

`-e`

Cuando se incluya este parámetro en la línea de comandos, iVMCLI usará un canal cifrado con SSL para transferir datos entre la estación de administración y el iDRAC6 en el sistema remoto. Si este parámetro no se incluye en la línea de comandos, la transferencia de datos no se cifra.

Opciones de shell de sistema operativo de iVMCLI

Las siguientes funciones del sistema operativo se pueden usar en la línea de comandos de iVMCLI:

- stderr/stdout redirection: redirige los mensajes impresos de la utilidad hacia un archivo.

  Por ejemplo, al utilizar el carácter mayor que (>), seguido de un nombre del archivo, se sobrescribe el archivo especificado con el mensaje impreso de la utilidad iVMCLI.

  NOTA: La utilidad iVMCLI no lee la entrada estándar (**stdin**). En consecuencia, la redirección de **stdin** no es necesaria.

- Ejecución en segundo plano: De manera predeterminada, la utilidad iVMCLI se ejecuta en primer plano. Utilice las funciones de shell de comandos del sistema operativo para hacer que la utilidad se ejecute en segundo plano. Por ejemplo, en los sistemas operativos Linux, el carácter (&) después del comando hace que el programa se genere como un nuevo proceso de segundo plano.

La última técnica es útil en programas de secuencias de comandos, ya que permite que esta secuencia de comandos proceda después de iniciado un nuevo proceso para el comando iVMCLI (de lo contrario, la secuencia de comandos se bloqueará hasta que el programa iVMCLI finalice). Cuando se inician varias instancias de iVMCLI de esta manera, y una o varias de las instancias de comando se terminan manualmente, utilice las instalaciones específicas del sistema operativo para enumerar y terminar los procesos.

Códigos de retorno de iVMCLI

0 = Sin errores

1 = No se puede conectar

2 = Error de línea de comandos de iVMCLI

3 = Se cerró la conexión del firmware del RAC

Cuando se presentan errores, también se envían mensajes de texto en inglés a la salida estándar de errores.

18

Uso de la utilidad de configuración del iDRAC6

Descripción general

La utilidad de configuración del iDRAC6 es un entorno de configuración previo al inicio que permite ver y establecer parámetros para iDRAC6 y para el sistema administrado. Específicamente, puede:

- Ver los números de revisión del firmware del iDRAC6 y del firmware de de plano posterior primario
- Configurar, activar o desactivar la red de área local (LAN) del iDRAC6
- Activar o desactivar la IPMI sobre LAN
- Configurar los parámetros de LAN
- Activar, desactivar o cancelar los servicios del sistema
- Activar o desactivar el descubrimiento automático y configurar el servidor de aprovisionamiento
- Conectar o desconectar los medios virtuales
- Activar o desactivar VFlash
- Activar o desactivar el inicio de sesión mediante tarjeta inteligente y el inicio de sesión único
- Configurar servicios del sistema
- Cambiar el nombre de usuario y la contraseña del administrador
- Restablecer la configuración predeterminada de fábrica del iDRAC6
- Ver o borrar los mensajes del registro de eventos del sistema (SEL)

Las tareas que puede realizar con la utilidad de configuración del iDRAC6 también pueden realizarse mediante otras utilidades que se incluyen con el iDRAC6 o el software Dell OpenManage, incluida la interfaz web, la interfaz de línea de comandos de SM-CLP, la interfaz de línea de comandos de RACADM local y remoto y, en el caso de la configuración de la red básica, en la pantalla LCD del iDRAC6 durante la configuración inicial del iDRAC6.

Inicio de la utilidad de configuración del iDRAC6

Se debe usar una consola conectada a la consola virtual de iDRAC6 para tener acceso a la utilidad de configuración del iDRAC6 al inicio o después de restablecer la configuración predeterminada del iDRAC6.

1. En el teclado conectado a la consola virtual del iDRAC6, presione <Impr Pant> para mostrar el menú **OSCAR (Configuración e informes en pantalla) de la consola virtual** de iDRAC6. Use la <flecha hacia arriba> y <flecha hacia abajo> para resaltar la ranura que contiene el servidor y después presiona <Intro>.
2. Encienda o reinicie el servidor con el botón de encendido que se encuentra en el frente del servidor.
3. Cuando aparezca el mensaje `Press <Ctrl-E> for Remote Access Setup within de 5 sec.....`, presione inmediatamente <Ctrl><E>. Aparece la utilidad de configuración del iDRAC6.

NOTA: Si el sistema operativo comienza a cargarse antes de que presione <Ctrl><E>, espere a que el sistema termine de iniciarse y luego reinicie el servidor e inténtelo otra vez.

Las dos primeras líneas de la utilidad de configuración ofrecen información sobre el firmware del iDRAC6 y las revisiones del firmware de plano posterior primario. Los niveles de revisión pueden ser útiles para determinar si necesita actualizar el firmware.

El firmware del iDRAC6 es la parte del firmware que se encarga de las interfaces externas, por ejemplo, la interfaz web, SM-CLP y las interfaces web. El firmware de plano posterior primario es la parte del firmware que se conecta con el entorno de hardware del servidor y lo supervisa.

Uso de la utilidad de configuración del iDRAC6

Bajo los mensajes de revisión de firmware, el resto de la utilidad de configuración del iDRAC6 es un menú de opciones a las que puede tener acceso por medio de las teclas de flecha ascendente y flecha descendente.

- Si un elemento del menú conduce a un submenú o a un campo de texto editable, presione <Intro> para acceder al elemento y <Esc> para salir de él después de terminar de configurarlo.

- Si un elemento tiene valores que se pueden seleccionar, como **Sí/No** o **Activado/Desactivado**, presione la flecha hacia la izquierda, la flecha hacia la derecha o la barra espaciadora para elegir un valor.
- Si un elemento no se puede editar, aparece en azul. Algunos elementos se pueden editar en función de otras selecciones que se hagan.
- La línea en la parte inferior de la pantalla muestra instrucciones relacionadas con el elemento actual. Puede presionar <F1> para mostrar la ayuda del elemento actual.
- Cuando haya terminado de usar la utilidad de configuración del iDRAC6, presione <Esc> para consultar el menú de salida, donde podrá elegir si desea guardar o descartar los cambios o volver a la utilidad.

Las siguientes secciones describen las opciones del menú de la utilidad de configuración del iDRAC6.

LAN del iDRAC6

Use la flecha hacia la izquierda, la flecha hacia la derecha y la barra espaciadora para seleccionar entre **Activado** y **Desactivado**.

La LAN del iDRAC6 está desactivada en la configuración predeterminada. Es necesario activar la LAN para permitir el uso de los servicios del iDRAC6 tales como la interfaz web, el acceso Telnet/SSH a la interfaz de línea de comandos de SM-CLP, la consola virtual y los medios virtuales.

Si elige desactivar la LAN, aparecerá la siguiente advertencia:

```
La interfaz del iDRAC fuera de banda se desactivará si
el canal de LAN está desactivado.
```

El mensaje le informa que, además de los servicios a los que tiene acceso a través de la conexión directa al iDRAC6 mediante HTTP, HTTPS, Telnet o los puertos SSH, el tráfico de red de administración fuera de banda, por ejemplo, los mensajes de IPMI que se envían al iDRAC6 desde una estación de administración, no se reciben cuando la LAN está desactivada. La interfaz RACADM local permanece disponible y se puede usar para reconfigurar la LAN del iDRAC6.

Presione cualquier tecla para quitar el mensaje y continuar.

IPMI en la LAN

Presione la tecla de flecha hacia la izquierda, la tecla de flecha hacia la derecha y la barra espaciadora para seleccionar entre **Activado** y **Desactivado**. Cuando se seleccione **Desactivado**, el iDRAC6 no aceptará mensajes IPMI que lleguen por medio de la interfaz de LAN.

Si elige **Desactivado**, aparecerá un mensaje de advertencia.

Presione cualquier tecla para quitar el mensaje y continuar. Para ver una explicación del mensaje, ver "LAN del iDRAC6" en la página 365.

Parámetros de la LAN

Presione <Intro> para mostrar el submenú de parámetros de la LAN. Cuando haya terminado de configurar los parámetros de la LAN, presione <Esc> para volver al menú anterior.

Tabla 18-1. Parámetros de la LAN

Elemento	Descripción
Valores comunes	
Dirección MAC	Ésta es la dirección MAC no editable de la interfaz de red del iDRAC6.
Activar VLAN	Muestra **Activado/Desactivado**. **Activado** permitirá el filtrado de LAN virtual para el iDRAC6.
Id. de VLAN	Muestra cualquier valor de identificación de VLAN entre 1 y 4094.
VLAN	Muestra la prioridad de la VLAN entre 0 y 7
Registrar el nombre del iDRAC6	Seleccione **Activado** para registrar el nombre del iDRAC6 en el servicio DNS. Seleccione **Desactivado** si no desea que los usuarios puedan encontrar el nombre del iDRAC6 en el DNS.
Nombre del iDRAC6	Si **Registrar el nombre del iDRAC** se encuentra **Activado**, presione <Intro> para modificar el campo de texto **Nombre actual del iDRAC de DNS**. Presione <Intro> cuando haya terminado de modificar el nombre del iDRAC6. Presione <Esc> para volver al menú anterior. El nombre del iDRAC6 debe ser un nombre de host DNS válido.

Tabla 18-1. Parámetros de la LAN *(continuación)*

Elemento	Descripción
Nombre de dominio de DHCP	Seleccione **Activado** si desea obtener el nombre de dominio de un servicio DHCP de la red. Seleccione **Desactivado** si desea especificar el nombre de dominio.
Nombre de dominio	Si **Nombre de dominio de DHCP** está **Desactivado**, presione <Intro> para modificar el campo de texto **Nombre de dominio actual**. Presione <Intro> cuando haya terminado de modificarlo. Presione <Esc> para volver al menú anterior. El nombre de dominio debe ser un dominio DNS válido, por ejemplo, `miempresa.com`.
Cadena del nombre del host	Presione <Intro> para editarla. Introduzca el nombre del host para alertas de captura de sucesos de plataforma (PET).
Alerta de LAN activada	Seleccione **Activado** para permitir un alerta de PET de LAN.
Entrada de política de alerta 1	Seleccione **Activar** o **Desactivar** para activar el primer destino de alerta.
Destino de alerta 1	Si **Alerta de LAN activada** está **Activada**, introduzca la dirección IP donde se enviarán las alertas de PET de LAN.
Configuración de IPv4	Active o desactive la compatibilidad para conexión IPv4.
IPv4	Seleccione **Activado** o **Desactivado** para la compatibilidad con el protocolo IPv4. El valor predeterminado es activado.
Clave de cifrado RMCP+	Presione <Intro> para modificar el valor, <Esc> cuando haya terminado. La clave de cifrado RMCP+ es una cadena hexadecimal de 40 caracteres (caracteres 0-9, a-f y A-F). RMCP+ es una extensión de IPMI que agrega la autentificación y el cifrado a IPMI. El valor predeterminado es una cadena de 40 ceros.

Tabla 18-1. Parámetros de la LAN *(continuación)*

Elemento	Descripción
Origen de dirección IP	Seleccione entre **DHCP** y **Estática**. Cuando se selecciona DHCP, los campos **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se obtienen de un servidor DHCP. Si no se encuentra ningún servidor DHCP en la red, los campos toman el valor cero. Cuando se selecciona **Estática**, las opciones **Dirección IP de Ethernet**, **Máscara de subred** y **Puerta de enlace predeterminada** se pueden editar.
Dirección IP de Ethernet	Si la opción **Fuente de dirección IP** se establece como **DHCP**, este campo muestra la dirección IP que se obtuvo de DHCP. Si la opción **Fuente de dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC6. La dirección predeterminada es **192.168.0.120.**
Máscara de subred	Si la opción **Fuente de dirección IP** se establece como **DHCP**, este campo muestra la dirección de máscara de subred que se obtuvo de DHCP. Si la opción **Fuente de dirección IP** se establece como **Estática**, introduzca la máscara de subred para el iDRAC6. El valor predeterminado es **255.255.255.0**.
Puerta de enlace predeterminada	Si **Fuente de dirección IP** se establece como **DHCP**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si **Fuente de dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada. El valor predeterminado es **192.168.0.1**.
Servidores DNS de DHCP	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidores DNS. Seleccione **Desactivado** para especificar las direcciones de servidores DNS a continuación.
Servidor DNS 1	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del primer servidor DNS.
Servidor DNS 2	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del segundo servidor DNS.
Configuración de IPv6	

Tabla 18-1. Parámetros de la LAN *(continuación)*

Elemento	Descripción
IPv6	Active o desactive la compatibilidad para la conexión IPv6.
Fuente de dirección IPv6	Seleccione entre **AutoConfig** y **Estática**. Cuando se selecciona **AutoConfig**, los campos **Dirección IPv6 1**, **Longitud del prefijo** y **Puerta de enlace predeterminada** se obtienen de DHCP. Cuando se selecciona **Estática**, las opciones **Dirección IPv6 1**, **Longitud del prefijo** y **Puerta de enlace predeterminada** se pueden editar.
Dirección IPv6 1	Si **Fuente de dirección IP** se establece como **AutoConfig**, este campo muestra la dirección IP que se obtuvo de DHCP. Si la opción **Fuente de dirección IP** se establece como **Estática**, introduzca la dirección IP que desea asignar al iDRAC6.
Longitud del prefijo	Configura la longitud del prefijo de la dirección IPv6. Puede ser un valor entre 1 y 128, inclusive.
Puerta de enlace predeterminada	Si **Fuente de dirección IP** se establece como **AutoConfig**, este campo mostrará la dirección IP de la puerta de enlace predeterminada que se obtuvo de DHCP. Si **Fuente de dirección IP** se establece como **Estática**, introduzca la dirección IP de la puerta de enlace predeterminada.
Dirección IPv6 de vínculo local	Ésta es la **dirección IPv6 de vínculo local** no editable de la interfaz de red del iDRAC6.
Dirección IPv6 2-15	Ésta es la **dirección IPv6 2... dirección IPv6 15** no editable de la interfaz de red del iDRAC6.
Servidores DNS de DHCPv6	Seleccione **Activado** para obtener de un servicio de DHCP en la red las direcciones de servidores DNS. Seleccione **Desactivado** para especificar las direcciones de servidores DNS a continuación.
Servidor DNS 1	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del primer servidor DNS.
Servidor DNS 2	Si **Servidores DNS de DHCP** está **Desactivado**, introduzca la dirección IP del segundo servidor DNS.

Configuración de soportes virtuales

Medios virtuales

Use la tecla de flecha hacia la izquierda y la tecla de flecha hacia la derecha para seleccionar las opciones **Conectado automáticamente**, **Conectado** o **Desconectado**.

- Si selecciona **Conectado**, los medios virtuales se conectan al bus USB y están listos para su uso durante las sesiones de **Consola virtual**.
- Si selecciona **Desconectado**, los usuarios no podrán acceder a los medios virtuales durante las sesiones de **Consola virtual**.
- Si selecciona **Conectado automáticamente**, los medios virtuales se conectan automáticamente al servidor al iniciar una sesión de medios virtuales.

NOTA: Para usar una unidad flash USB con la función de Medios virtuales, debe establecer la opción **Tipo de emulación de unidad flash USB** como **Disco duro** en la utilidad de configuración del BIOS. Se accede a la utilidad de configuración del BIOS al presionar <F2> durante el arranque del servidor. Si el **Tipo de emulación de la unidad flash USB** se establece como **Automático**, la unidad flash aparecerá como unidad de disco flexible en el sistema.

vFlash

Use la tecla de flecha hacia la izquierda y la tecla de flecha hacia la derecha para seleccionar **Activado** o **Desactivado**.

- **Activado:** vFlash está disponible para la administración de particiones.
- **Desactivado**: vFlash no está disponible para la administración de particiones.

PRECAUCIÓN: vFlash no se puede desactivar si una o más particiones están en uso o están conectadas.

Initialize vFlash

Elija esta opción para inicializar la tarjeta vFlash. La operación de inicialización borra los datos existentes en la tarjeta SD y todas las particiones existentes se eliminan. No puede realizar una operación de inicialización si una o más particiones están en uso o conectadas. Esta opción es accesible sólo si una tarjeta de un tamaño mayor que 256 MB está presente en la ranura para tarjeta de iDRAC Enterprise y si vFlash está activado.

Presione <Intro> para inicializar la tarjeta vFlash SD.

La operación de inicialización puede fallar debido a los siguientes motivos:

- La tarjeta SD no está presente actualmente.
- vFlash está siendo utilizado actualmente por otro proceso.
- vFlash no está activado.
- La tarjeta SD está protegida contra escritura.
- Una o más particiones están en uso actualmente.
- Una o más particiones están conectadas actualmente.

Propiedades de vFlash

Presione <Intro> para ver las siguientes propiedades de la tarjeta vFlash SD:

- **Nombre**: muestra el nombre de la tarjetavFlash SD insertada en la ranura para tarjeta vFlash SD del servidor. Si es una tarjeta SD Dell, dirá "vFlash SD Card". Si es una tarjeta SD que no es de Dell, dirá "SD Card".
- **Tamaño**: muestra el tamaño de la tarjeta vFlash SD en gigabytes (GB).
- **Espacio disponible**: muestra el espacio no utilizado en la tarjeta vFlash SD en megabytes (MB). Este espacio está disponible para crear más particiones en la tarjeta vFlash SD. Para las tarjetas SD, el espacio disponible aparece como 256 MB.
- **Protegido contra escritura**: muestra si la tarjeta vFlash SD está protegida contra escritura o no.
- **Condición**: muestra la condición general de la tarjeta vFlash SD. Ésta puede ser:
  - En buen estado
  - Aviso
  - Critical (Crítico)

Presione <Esc> para salir.

Tarjeta inteligente/SSO

Esta opción configura las funciones **Inicio de sesión mediante tarjeta inteligente** e **Inicio de sesión único**. Las opciones disponibles son **Activado** y **Desactivado**.

NOTA: Si activa la función **Inicio de sesión único**, se desactivará la función **Inicio de sesión mediante tarjeta inteligente**.

Servicios del sistema

Servicios del sistema

Use la tecla de flecha hacia la izquierda y la tecla de flecha hacia la derecha para seleccionar **Activado** o **Desactivado**. Si están activadas, algunas funciones de iDRAC6 pueden configurarse a través de Lifecycle Controller. Para obtener más información, consulte la *Lifecycle Controller User Guide* (Guía del usuario de Lifecycle Controller), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

NOTA: Si modifica esta opción, el servidor se reiniciará cuando presione **Guardar** y **Salir** para aplicar la nueva configuración.

Cancelación de servicios del sistema

Use la tecla de flecha hacia arriba y la tecla de flecha hacia abajo para seleccionar **Sí** o **No**.

Al seleccionar **Sí**, se cierran todas las sesiones de Lifecycle Controller y el servidor se reinicia al presionar **Guardar** y **Salir** para aplicar la nueva configuración.

Recopilar el inventario del sistema en el reinicio

Seleccione la opción **Activado** para permitir la recopilación del inventario durante el reinicio. Para obtener más información, consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

NOTA: Si esta opción se modifica, el servidor se reiniciará después de guardar la configuración y salir de la utilidad de configuración del iDRAC6.

Configuración de usuario de LAN

El usuario de la LAN es la cuenta de administrador del iDRAC6, que tiene el nombre predeterminado **root**. Presione <Intro> para mostrar el submenú de configuración de usuario de LAN. Cuando haya terminado de configurar el usuario de LAN, presione <Esc> para volver al menú anterior.

Tabla 18-2. Pantalla de configuración de usuarios de la LAN

Elemento	Descripción
Descubrimiento automático	El descubrimiento automático permite descubrir automáticamente sistemas no aprovisionados en la red y establece *de manera segura* las credenciales iniciales para administrar estos sistemas. Esta función permite al iDRAC6 localizar el servidor de aprovisionamiento. El iDRAC6 y el servidor de servicio de aprovisionamiento se autentifican el uno al otro. El servidor de aprovisionamiento remoto envía las credenciales del usuario para que el iDRAC6 genere una cuenta de usuario con esas credenciales. Una vez creada la cuenta de usuario, una consola remota puede establecer una comunicación WSMAN con el iDRAC6 utilizando las credenciales especificadas en el proceso de descubrimiento y luego enviar instrucciones seguras al iDRAC6 para implementar un sistema operativo de manera remota. Para obtener información sobre la implementación remota del sistema operativo, consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**. Lleve a cabo los siguientes pasos previos en una sesión *independiente* de la **utilidad de configuración del iDRAC6** *antes de activar manualmente el descubrimiento automático*: • Activar el NIC (servidores blade) • Activar IPv4 (servidores blade) • Activar DHCP • Obtener el nombre de dominio de DHCP • Desactivar la cuenta de administrador (cuenta n.º 2) • Obtener la dirección de servidor DNS desde DHCP • Obtener el nombre de dominio DNS de DHCP Seleccionar **Activado** para activar la función del descubrimiento automático. De manera predeterminada, la opción aparece como **desactivado**. Si solicitó un sistema Dell con la función del descubrimiento automático **Activado**, el iDRAC6 del sistema Dell se suministrará con DHCP activado sin credenciales predeterminadas para un inicio de sesión remoto.

Tabla 18-2. Pantalla de configuración de usuarios de la LAN *(continuación)*

Elemento	Descripción
Descubrimiento automático *(continuación)*	Antes de agregar el sistema Dell a la red y utilizar la función de descubrimiento automático, verifique los siguientes datos: • El servidor del protocolo de configuración dinámica de host (DHCP) y el sistema de nombres de dominio (DNS) están configurados. • Los servicios web de aprovisionamiento están instalados, configurados y registrados.
Servidor de aprovisionamiento	Este campo se utiliza para configurar el servidor de aprovisionamiento. La dirección del servidor de aprovisionamiento puede ser una combinación de direcciones IPv4 o nombres de host y no debe superar los 255 caracteres. Cada dirección o nombre de host debe separarse por medio de una coma. Si activó la función de descubrimiento automático, las credenciales de usuario se obtienen del servidor de aprovisionamiento configurado para permitir el aprovisionamiento remoto en el futuro después de completar el proceso de descubrimiento automático correctamente. Para obtener más información, consulte la *Dell Lifecycle Controller User Guide* (Guía del usuario de Dell Lifecycle Controller), disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.
Acceso a la cuenta	Seleccione **Activado** para activar la cuenta de administrador. Seleccione la opción **Desactivado** para desactivar la cuenta del administrador o en caso de que el descubrimiento automático está activado.
Privilegio LAN de IPMI	Seleccione **Admin**, **Usuario**, **Operador** o **Sin acceso**.
Nombre de usuario de la cuenta	Presione <Intro> para modificar el nombre de usuario y presione <Esc> cuando haya terminado. El nombre de usuario predeterminado es **root**.
Introducir la contraseña	Introduzca la contraseña nueva para la cuenta de administrador. Los caracteres no aparecerán en la pantalla cuando usted los introduzca.

Tabla 18-2. Pantalla de configuración de usuarios de la LAN *(continuación)*

Elemento	Descripción
Confirm Password (Confirmar la contraseña)	Introduzca nuevamente la nueva contraseña para la cuenta de administrador. Si los caracteres no coinciden con los caracteres que introdujo en el campo **Introducir la contraseña**, aparecerá un mensaje y usted deberá introducir nuevamente la contraseña.

Restablecer valores predeterminados

Use la opción de menú **Restablecer valores predeterminados** para restablecer todos los valores predeterminados de fábrica de las opciones de configuración del iDRAC6. Esto puede ser necesario, por ejemplo, cuando usted ha olvidado la contraseña del usuario administrativo o si desea volver a configurar el iDRAC6 a partir de la configuración predeterminada.

NOTA: En la configuración predeterminada, el sistema de red del iDRAC6 está desactivado. Usted no podrá reconfigurar el iDRAC6 por medio de la red hasta que haya activado la red del iDRAC6 en la utilidad de configuración del iDRAC6.

Presione <Intro> para seleccionar el elemento. Aparece el mensaje de advertencia siguiente:

```
Si restablece los valores predeterminados de fábrica
restaura la configuración no volátil de usuario
remoto. ¿Continuar?

< NO (Cancelar) >

< SÍ (Continuar) >
```

Para restablecer los valores predeterminados de iDRAC6, seleccione **SÍ** y presione <Intro>.

Cualquiera de los mensajes de error siguientes aparece si esta operación falla:

- El comando de restablecimiento no fue satisfactorio. Por favor intente más tarde, el iDRAC está ocupado.
- No fue posible restablecer la configuración a los valores predeterminados; fin del tiempo de espera.
- No es posible enviar el comando Restablecer. Por favor intente más tarde, el iDRAC está ocupado.

Menú del registro de sucesos del sistema

El menú **Registro de sucesos del sistema** permite ver y borrar los mensajes del registro de sucesos del sistema (SEL). Presione <Intro> para mostrar el **Menú del registro de sucesos del sistema**. El sistema cuenta las entradas del registro y después muestra el número total de entradas y el mensaje más reciente. El SEL retiene un máximo de 512 mensajes.

Para ver los mensajes del registro de sucesos del sistema, seleccione **Ver registro de sucesos del sistema** y presione <Intro>. Para desplazarse:

- Use la flecha hacia la izquierda para retroceder al mensaje anterior (más antiguo) y la flecha hacia la derecha para avanzar al mensaje siguiente (más reciente).
- Introduzca un número de registro específico para ir directamente al registro.

Presione <Esc> para salir del Registro de sucesos del sistema.

NOTA: Sólo puede borrar el registro de sucesos del sistema en la utilidad de configuración del iDRAC6 o en la interfaz web del iDRAC6.

Para borrar el SEL, seleccione **Borrar el registro de sucesos del sistema** y presione <Intro>.

Cuando haya terminado con el menú del SEL, presione <Esc> para volver al menú anterior.

Cómo salir de la utilidad de configuración del iDRAC6

Cuando haya terminado de hacer cambios en la configuración del iDRAC6, presione la tecla <Esc> para mostrar el menú de salida.

- Seleccione **Guardar cambios y salir** y presione <Intro> para retener los cambios. Si esta operación falla, aparece uno de los siguientes mensajes:
  - Falla de comunicación del iDRAC6: Se muestra si no se puede acceder al iDRAC.
  - No se pueden aplicar algunos de los valores: Se muestra cuando no se pueden aplicar algunos de los valores.
- Seleccione **Descartar cambios y salir** y presione <Intro> para ignorar los cambios que ha realizado.
- Seleccione **Regresar a la configuración** y presione <Intro> para volver a la utilidad de configuración del iDRAC6.

19

Recuperación y solución de problemas del sistema administrado

Esta sección explica cómo realizar las tareas relacionadas con los diagnósticos y solución de problemas de un sistema administrado remoto por medio de las utilidades del iDRAC6. Contiene las siguientes subsecciones:

- Indicadores de problemas: Ayuda a encontrar mensajes y otros indicadores del sistema que pueden conducir a un diagnóstico del problema
- Herramientas para solución de problemas: Describe las herramientas de iDRAC6 que se pueden usar para solucionar problemas del sistema
- Solución de problemas y preguntas frecuentes: Respuestas a situaciones típicas que podría enfrentar

La seguridad primero, para el usuario y para el sistema

Para realizar ciertos procedimientos de esta sección, debe trabajar con el chasis, con el sistema Dell PowerEdge o con otros módulos de hardware. No trate de reparar el hardware del sistema salvo cuando se explique en esta guía o en la documentación del sistema.

PRECAUCIÓN: Muchas de las reparaciones sólo pueden realizarlas los técnicos de servicio autorizados. Sólo realice las soluciones de problemas y reparaciones sencillas autorizadas en la documentación del producto o según lo indique el equipo de servicio y asistencia técnica por teléfono o en línea. La garantía no cubre los daños ocasionados por reparaciones que Dell no haya autorizado. Lea y siga las instrucciones de seguridad entregadas con el producto.

Indicadores de problemas

Esta sección describe indicadores que sugieren que puede haber un problema en el sistema.

Indicadores LED

Los indicadores LED del chasis o de los componentes instalados en el chasis son generalmente los primeros indicadores de problemas en el sistema. Los siguientes componentes y módulos tienen indicadores LED de estado:

- Pantalla LCD del chasis
- Servidores
- Ventiladores
- CMC
- Módulos de E/S
- Suministros de energía

El indicador LED de la pantalla LCD del chasis resume el estado de todos los componentes del sistema. Un LED de color azul indica que no se han detectado condiciones de falla en el sistema. Si el LED parpadea en color ámbar, indica que se han detectado una o más condiciones de falla.

Si la pantalla LCD del chasis tiene un LED que parpadea en color ámbar, se puede usar el menú de la pantalla LCD para encontrar el componente que tiene la falla. Consulte la *Guía del usuario de firmware de Dell Chassis Management Controller* para obtener ayuda respecto del uso de la pantalla LCD.

La Tabla 19-1 describe el significado del comportamiento del indicador LED del sistema Dell PowerEdge:

Tabla 19-1. Indicadores LED del servidor blade

Indicador LED	Significado
verde continuo (*sólo para el botón de encendido*)	El servidor está encendido. La ausencia del indicador LED en color verde significa que el servidor no está encendido.
azul continuo	El iDRAC6 presenta una condición satisfactoria.
parpadeo en color ámbar	El iDRAC6 ha detectado una condición de falla o es posible que esté en proceso de actualizar el firmware.
parpadeo en color azul	Un usuario ha activado la identificación de localizador de este servidor.

Indicadores de problemas del hardware

Los indicadores de que un módulo tiene un problema de hardware incluyen los siguientes:

- Falla de encendido
- Ventiladores ruidosos
- Pérdida de conectividad de red
- Alertas de los sensores de supervisión de la batería, temperatura, voltaje o alimentación
- Fallas de disco duro
- Falla de soportes USB
- Daños físicos provocados por caídas, agua u otros agentes externos

Cuando se presentan estos tipos de problemas, inspeccione el daño causado e intente corregir el problema con estas estrategias:

- Vuelva a insertar el módulo y reinícielo
- Inserte el módulo en otro compartimiento del chasis
- Sustituya los discos duros o memorias USB
- Vuelva a conectar o reemplace los cables de alimentación y de red

Si estos pasos no corrigen el problema, consulte el *Manual del propietario del hardware* para obtener información específica para la solución de problemas del dispositivo de hardware.

Otros indicadores de problemas

Tabla 19-2. Indicadores de problemas

Buscar:	Acción:
Mensajes de alerta procedentes del software de administración de sistemas	Consulte la documentación del software de administración de sistemas.
Mensajes en el registro de sucesos del sistema	Vea la "Consulta del registro de sucesos del sistema (SEL)" en la página 381.
Mensajes del código de la POST del inicio	Vea la "Verificar los códigos de la POST" en la página 383.
Mensajes en la pantalla de último bloqueo	Vea la "Visualización de la pantalla de último bloqueo del sistema" en la página 383.

Tabla 19-2. Indicadores de problemas *(continuación)*

Buscar:	Acción:
Mensajes de alerta en la pantalla de estado del servidor de la LCD	Vea la "Consulta de la pantalla de estado del servidor en busca de mensajes de error" en la página 386.
Mensajes en el registro del iDRAC6	Vea la "Visualización del registro del iDRAC6" en la página 396.

Herramientas para solución de problemas

Esta sección describe las utilidades del iDRAC6 que se pueden usar para diagnosticar problemas del sistema, sobre todo cuando se tratan de solucionar de manera remota.

- Verificar la condición del sistema
- Consultar el registro de sucesos del sistema en busca de mensajes de error
- Consultar los códigos de la POST
- Visualización de la pantalla de último bloqueo
- Visualización de las secuencias de inicio más recientes
- Consulta de la pantalla de estado del servidor en la pantalla LCD en busca de mensajes de error
- Visualización del registro del iDRAC6
- Visualización de la información del sistema
- Identificación del servidor administrado en el chasis
- Uso de la consola de diagnósticos
- Administración de la alimentación en un sistema remoto

Consulta de la condición del sistema

Al iniciar sesión en la interfaz web del iDRAC6, la pantalla **Resumen del sistema** muestra la condición de los componentes del sistema.La Tabla 19-3 describe el significado de los indicadores de condición del sistema.

Tabla 19-3. Indicadores de la condición del servidor

Indicador	Descripción
	Una marca de verificación verde indica una condición de estado satisfactoria (normal).
	Un triángulo amarillo que contiene un signo de exclamación indica una condición de estado de advertencia (no crítica).
	Una X roja indica una condición de estado crítica (falla).
	Un icono con un signo de interrogación indica que se desconoce el estado.

Haga clic en cualquier componente en la sección **Condición del servidor** para ver la información acerca del componente. Se muestran las lecturas de sensores de baterías, temperaturas, voltajes y supervisión de alimentación, lo que ayuda a diagnosticar algunos tipos de problemas. Las pantallas de información del iDRAC6 y el CMC muestran información útil sobre el estado actual y la configuración.

Consulta del registro de sucesos del sistema (SEL)

La pantalla **Registro SEL** muestra los mensajes de los sucesos que ocurren en el servidor administrado.

Para ver el **Registro de sucesos del sistema**, realice los pasos a continuación:

1. Haga clic en **Sistema** y después haga clic en la ficha **Registros**.
2. Haga clic en **Registro de sucesos del sistema** para mostrar la pantalla **Registro de sucesos del sistema**.

   La pantalla **Registro de sucesos del sistema** muestra un indicador de condición del sistema (ver Tabla 19-3), la fecha y hora, así como una descripción del suceso.
3. Haga clic en el botón **Registro de sucesos del sistema** correspondiente para continuar (ver Tabla 19-4).

Tabla 19-4. Botones del registro de sucesos del sistema

Botón	Acción
Borrar registro	Borra el registro de sucesos del sistema. **NOTA:** El botón **Borrar registro** sólo aparece si tiene permiso para **Borrar registros**.

Tabla 19-4. Botones del registro de sucesos del sistema *(continuación)*

Botón	Acción
Guardar como	Abre una ventana emergente que le permite guardar el registro de sucesos del sistema en el directorio de su elección. **NOTA:** Si al usar Internet Explorer tiene un problema para guardar, asegúrese de descargar la actualización de seguridad acumulada para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en **support.microsoft.com**. **NOTA:** Si cuando usa Internet Explorer, no puede guardar el registro de sucesos del sistema utilizando **Guardar como**, puede deberse a la configuración del explorador. Para resolver esto: **1** En Internet Explorer, vaya a **Herramientas→ Opciones de Internet→ Seguridad** y seleccione la zona en la que intenta descargar. Por ejemplo, si el dispositivo iDRAC está en la Intranet local, seleccione **Intranet local** y haga clic en **Nivel personalizado**... **2** En la ventana **Configuración de seguridad**, en **Descargas** compruebe que las siguientes opciones están activadas: • Preguntar automáticamente si se debe descargar un archivo • Descarga de archivos **PRECAUCIÓN: Para garantizar que el equipo usado para acceder al iDRAC es seguro, en *Varios*, no debe estar activada la opción *Inicialización de aplicaciones y archivos inseguros*.**
Advanced Settings (Configuración avanzada)	Abre la página **Configuración avanzada del Registro de eventos del sistema** que le permite activar/desactivar los mensajes de eventos de OEM desde el sistema administrado que se muestra en el SFL. Haga clic en **Aplicar** para aplicar la configuración.

Uso de la línea de comandos para ver el Registro de eventos del sistema

El comando es:

```
racadm getsel <options>
```

Si no se especifican argumentos, se muestra todo el registro.

Para mostrar el número de entradas de SEL:

```
racadm getsel -i
```

NOTA: Para obtener más información sobre las opciones, consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

El comando `clrsel` elimina todos los registros existentes del SEL.

```
racadm clrsel
```

Verificar los códigos de la POST

La pantalla **Códigos de la POST** muestra el último código de la POST del sistema antes de iniciar el sistema operativo. Los códigos de la POST son indicadores de progreso del sistema BIOS que indican varias etapas de la secuencia de inicio desde el restablecimiento de la alimentación, y permiten diagnosticar fallas relacionadas al inicio del sistema.

NOTA: Vea el texto para conocer los números de mensaje de códigos de la POST en la pantalla LCD o en el *Manual del propietario del hardware.*

Para ver los códigos de la POST, haga clic en **Sistema→ Registros→ Código de la POST**. La pantalla **Código de la POST** muestra un indicador de condición del sistema (ver Tabla 19-3), un código hexadecimal y una descripción del código.

Visualización de la pantalla de último bloqueo del sistema

NOTA: La función de pantalla de último bloqueo se debe configurar en Server Administrator y en la interfaz web del iDRAC6. Ver "Configuración del servidor administrado para capturar la pantalla de último bloqueo" en la página 86 para obtener instrucciones sobre cómo configurar esta función.

La **Pantalla de último bloqueo** muestra la pantalla del bloqueo más reciente, que incluye información acerca de los sucesos que ocurrieron antes de que el sistema se bloqueara. La imagen del último bloqueo del sistema se guarda en el almacén persistente del iDRAC6 y se puede acceder a ella de manera remota. La pantalla de último bloqueo aparece disponible incluso si iDRAC se restablece ya que se encuentra almacenada en la NVRAM.

Para ver la **Pantalla de último bloqueo**, haga clic en **Sistema→ Registros→ Pantalla del último bloqueo**. La **Pantalla de último bloqueo** muestra la última pantalla de bloqueo guardada.

Haga clic en **Guardar** para guardar la pantalla de último bloqueo a un directorio de su elección.

Haga clic en **Eliminar** para borrar la pantalla de último bloqueo.

NOTA: Los botones **Guardar** y **Eliminar** no aparecerán si no hay ninguna pantalla de bloqueo guardada.

NOTA: Debido a fluctuaciones en el temporizador de recuperación automática, es posible que la **pantalla de último bloqueo** no pueda capturarse cuando el temporizador de restablecimiento del sistema tenga un valor demasiado alto. El valor predeterminado es de 480 segundos. Utilice Server Administrator o IT Assistant para definir el temporizador de restablecimiento del sistema en 60 segundos y para asegurarse de que la **pantalla de último bloqueo** funcione correctamente. Consulte "Configuración del servidor administrado para capturar la pantalla de último bloqueo" en la página 86 para obtener información adicional.

Visualización de las secuencias de inicio más recientes

Si experimenta problemas de inicio, puede ver la actividad de pantalla de lo sucedido durante las últimas tres secuencias de inicio desde la pantalla **Captura de inicio**. La reproducción de las pantallas de inicio ocurre a una velocidad de 1 marco por segundo. El iDRAC6 registra cincuenta marcos durante el tiempo de inicio. Si el iDRAC se restablece, el vídeo de captura de inicio no está disponible ya que está almacenado en la memoria RAM y se elimina cuando el iDRAC se restablece.

La Tabla 19-5 presenta una lista de las acciones de control disponibles.

NOTA: Debe disponer de privilegios de administrador para ver la reproducción de las secuencias de captura de inicio.

Tabla 19-5. Opciones de captura de inicio

Botón/Opción	Descripción
Selecciona la secuencia de inicio	Permite seleccionar la secuencia de inicio a cargar y reproducir. • Captura de inicio 1: Carga la secuencia de inicio más reciente. • Captura de inicio 2: Carga la (segunda) secuencia de inicio que ocurrió antes de la captura de inicio 1. • Captura de inicio 3: Carga la (tercera) secuencia de inicio que ocurrió antes de la captura de inicio 2.

Tabla 19-5. Opciones de captura de inicio *(continuación)*

Botón/Opción	Descripción
Guardar como	Crea un archivo .zip comprimido que contiene todas las imágenes de captura de inicio de la secuencia actual. El usuario debe disponer de privilegios de administrador para realizar esta acción.
Pantalla anterior	Lo lleva a la pantalla anterior, de existir, en la consola de reproducción.
Reproducir	Inicia la reproducción de la pantalla actual en la consola de reproducción.
Pause	Interrumpe la reproducción en la pantalla actual que se está mostrando en la consola de reproducción.
Detener	Detiene la reproducción de pantalla y carga la primera pantalla de esa secuencia de inicio.
Pantalla siguiente	Lo lleva a la pantalla siguiente, de existir, en la consola de reproducción.
Imprimir	Imprime la imagen de la captura de inicio que aparece en la pantalla.
Refresh (Actualizar)	Vuelve a cargar la pantalla de la captura de inicio.

Visualización y adición de notas de trabajo

La página **Notas de trabajo** muestra las entradas de la nota de trabajo almacenadas en el Registro Lifecycle. Para ver la página **Notas de trabajo**, expanda el árbol del **Sistema** y haga clic en **Sistemas→ Registros→ Notas de trabajo**.

Se mostrará la marca de tiempo grabada en cada entrada de nota de trabajo y los contenidos de la nota de trabajo. El formato de la marca de tiempo es yyyy/mm/dd hh:mm:ss, según el horario de 24 horas.

Cada usuario que inicie sesión en iDRAC puede agregar notas de trabajo al registro. Se admite un máximo de 50 caracteres para cada nota de trabajo nueva. Haga clic en **Guardar** para agregar la nota al registro.

NOTA: Puede usar caracteres especiales excepto '<' y '&'. Si usa estos caracteres, no podrá guardar la nota de trabajo.

NOTA: Para poder agregar notas de trabajo debe contar con privilegios de inicio de sesión en iDRAC. Ver "Cómo agregar y configurar usuarios del iDRAC6" en la página 104 para obtener ayuda con la configuración de permisos de usuario.

Consulta de la pantalla de estado del servidor en busca de mensajes de error

Cuando un indicador LED parpadea en color ámbar y un servidor específico tiene un error, la pantalla de estado del servidor principal en la pantalla LCD resaltará el servidor afectado con un color naranja. Use los botones de navegación de la pantalla LCD para resaltar el servidor afectado y después haga clic en el botón central. Los mensajes de error y advertencia aparecerán en la segunda línea. La tabla siguiente muestra una lista de todos los mensajes de error y la gravedad de los mismos.

Tabla 19-6. Pantalla de estado del servidor

Gravedad	Message (Mensaje)	Causa
Aviso	Temperatura ambiente de la placa del sistema: Sensor de temperatura de la placa del sistema, suceso de advertencia	La temperatura ambiente del servidor superó el umbral de advertencia
Critical (Crítico)	Temperatura ambiente de la placa del sistema: Sensor de temperatura de la placa del sistema, suceso de falla	La temperatura ambiente del servidor superó el umbral de falla
Critical (Crítico)	Batería CMOS de la placa del sistema: Sensor de la batería de la placa del sistema, se confirmó una falla	No hay batería CMOS o no tiene voltaje
Aviso	Nivel de sistema de la placa del sistema: Sensor de corriente de la placa del sistema, suceso de advertencia	La corriente superó un umbral de advertencia
Critical (Crítico)	Nivel de sistema de la placa del sistema: Sensor de corriente de la placa del sistema, suceso de falla	La corriente superó un umbral de falla

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	CPU<número> <nombre del sensor de voltaje>:<número> sensor de voltaje de la CPU, se confirmó el estado declarado	Voltaje fuera de rango
Critical (Crítico)	<Nombre del sensor de voltaje> de la placa del sistema: Sensor de voltaje de la placa del sistema, se confirmó el estado declarado	Voltaje fuera de rango
Critical (Crítico)	CPU<número> <nombre del sensor de voltaje>:<número> sensor de voltaje de la CPU, se confirmó el estado declarado	Voltaje fuera de rango
Critical (Crítico)	Estado de la CPU<número>: Sensor de procesador de la CPU<número>, se confirmó el IERR	Falla de la CPU
Critical (Crítico)	Estado de la CPU<número>: Sensor de procesador de la CPU<número>, se confirmó un disparo térmico	La CPU se sobrecalentó
Critical (Crítico)	Estado de la CPU<número>: Sensor de procesador de la CPU<número>, se confirmó un error de configuración	Tipo incorrecto de procesador o instalación en el lugar erróneo
Critical (Crítico)	Estado de la CPU<número>: Sensor de procesador de la CPU<número>, no se confirmó la presencia	La CPU requerida no se encuentra o no está presente
Critical (Crítico)	Tarjeta elevadora de vídeo de la placa del sistema: Sensor de módulo de la placa del sistema, se confirmó el retiro del dispositivo	Se retiró el módulo requerido

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	Estado de la tarjeta mezzanine B<número de ranura>: Sensor de tarjeta de complemento para la tarjeta mezzanine B<número de ranura>, se confirmó un error de instalación	Tarjeta mezzanine incorrecta instalada para la red Fabric de E/S
Critical (Crítico)	Estado de la tarjeta mezzanine B<número de ranura>: Sensor de tarjeta de complemento para la tarjeta mezzanine B<número de ranura>, se confirmó un error de instalación	Tarjeta mezzanine incorrecta instalada para la red Fabric de E/S
Critical (Crítico)	Unidad de plano posterior <número>: Sensor de ranura de unidad del plano posterior, se retiró la unidad	Se retiró la unidad de almacenamiento
Critical (Crítico)	Unidad de plano posterior <número>: Sensor de ranura de unidad del plano posterior, se confirmó una falla de la unidad	Falló la unidad de almacenamiento
Critical (Crítico)	Protección contra fallas PFault de la placa del sistema: Sensor de voltaje de la placa del sistema, se confirmó el estado declarado	Este suceso se genera cuando los voltajes de la placa del sistema no se encuentran en los niveles normales
Critical (Crítico)	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó que el temporizador expiró	El temporizador de vigilancia de iDRAC6 expiró y no se estableció ninguna acción
Critical (Crítico)	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó un reinicio	La vigilancia de iDRAC6 detectó que el sistema se ha bloqueado (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de reiniciar

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó el apagado	La vigilancia de iDRAC6 detectó que el sistema se ha bloqueado (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de apagado
Critical (Crítico)	Vigilancia del sistema operativo de la placa del sistema: Sensor de vigilancia de la placa del sistema, se confirmó un ciclo de encendido	La vigilancia de iDRAC6 detectó que el sistema se ha bloqueado (el temporizador expiró porque no se recibió respuesta del host) y se estableció la acción de ciclo de encendido
Critical (Crítico)	Registro de sucesos de la placa del sistema: Sensor de registro de sucesos de la placa del sistema, se confirmó que el registro está lleno	El dispositivo de registro de sucesos del sistema detecta que sólo se podrá agregar una entrada al registro antes de que se llene
Aviso	Error corregible ECC: Sensor de memoria, el ECC corregible (<ubicación del DIMM>) se confirmó	Los errores ECC corregibles alcanzaron una frecuencia crítica
Critical (Crítico)	Error incorregible de ECC: un ECC incorregible (<ubicación del DIMM>) se confirmó	Se detectó un error ECC incorregible
Critical (Crítico)	Rev. de canal de E/S: Sensor de sucesos críticos, se confirmó una NMI de revisión de canal de E/S	Se genera una interrupción crítica en el canal de E/S
Critical (Crítico)	Error de paridad de PCI: Sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de paridad en el bus PCI
Critical (Crítico)	Error de sistema de PCI: Sensor de sucesos críticos, se confirmó un SERR de PCI (<número de ranura o id. de dispositivo PCI>)	El dispositivo detectó un error de PCI

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	Registro SBE desactivado: Sensor de registro de sucesos, se confirmó la desactivación del registro de errores corregibles de memoria	El registro de errores de un solo bit se desactiva cuando se registran demasiados SBE (errores de un solo bit)
Critical (Crítico)	Desactivación de registro: Sensor del registro de sucesos, se confirmó la desactivación del registro de todos los sucesos	Se desactivó el registro de todos los errores
No recuperable	Error de protocolo de CPU: Sensor de procesador, se confirmó la transición a estado no recuperable	El protocolo del procesador ingresó a un estado no recuperable
No recuperable	PERR de bus de CPU: Sensor de procesador, se confirmó la transición a un estado no recuperable	El PERR de bus del procesador ingresó a un estado no recuperable
No recuperable	Error de inicialización de CPU: Sensor de procesador, se confirmó la transición a un estado no recuperable	La inicialización del procesador ingresó a un estado no recuperable
No recuperable	Revisión de máquina de CPU: Sensor de procesador, se confirmó la transición a un estado no recuperable	La revisión de máquina del procesador ingresó a un estado no recuperable
Critical (Crítico)	Repuesto de memoria: Sensor de memoria, redundancia perdida (<ubicación del DIMM>) se confirmó	El repuesto de la memoria ya no es redundante
Critical (Crítico)	Memoria reflejada: Sensor de memoria, redundancia perdida (<ubicación del DIMM>) se confirmó	La memoria reflejada ya no es redundante

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	RAID de memoria: Sensor de memoria, redundancia perdida (<ubicación del DIMM>) se confirmó	La memoria de RAID ya no es redundante
Aviso	Se agregó memoria: Sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>)	Se retiró el módulo de memoria agregado
Aviso	Se quitó la memoria: Sensor de memoria, no se confirmó la presencia (<ubicación del DIMM>)	Se retiró el módulo de memoria
Critical (Crítico)	Error de configuración de memoria: Sensor de memoria, un error de configuración (<ubicación del DIMM>) se confirmó	La configuración de la memoria no es correcta para el sistema
Aviso	Ganancia de redundancia de memoria: Sensor de memoria, redundancia degradada (<ubicación del DIMM>) se confirmó	La redundancia de la memoria se ha degradado pero no se ha perdido
Critical (Crítico)	Error fatal de PCIE: sensor de sucesos críticos, se confirmó un error fatal de bus	Se detectó un error fatal en el bus de PCIE
Critical (Crítico)	Error de chipset: Sensor de sucesos críticos, se confirmó un PERR de PCI	Se detectó un error de chip
Aviso	Advertencia de memoria ECC: Sensor de memoria, se confirmó la transición de buen estado a estado no crítico (<ubicación del DIMM>)	Los errores corregibles ECC han aumentado por encima de la frecuencia normal

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	Advertencia de memoria ECC: Sensor de memoria, se confirmó la transición de un estado crítico a uno menos grave (<ubicación del DIMM>)	Los errores ECC corregibles han alcanzado una frecuencia crítica
Critical (Crítico)	Error de la POST: Sensor de la POST, no hay memoria instalada	No se detectó memoria en la placa
Critical (Crítico)	Error de la POST: Sensor de la POST, error de configuración de memoria	Se ha detectado la memoria, pero no se puede configurar
Critical (Crítico)	Error de la POST: Sensor de la POST, error de memoria inutilizable	Se ha configurado la memoria, pero no se puede utilizar
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la caché rápida del BIOS	Falla de la caché rápida del BIOS del sistema
Critical (Crítico)	Error de la POST: Sensor de la POST, falló el CMOS	Error de CMOS
Critical (Crítico)	Error de la POST: Sensor de la POST, falló el controlador DMA	Error del controlador DMA
Critical (Crítico)	Error de la POST: Sensor de la POST, falló el controlador de interrupción	Falla del controlador de interrupción
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la actualización del temporizador	Error de actualización del temporizador
Critical (Crítico)	Error de la POST: Sensor de la POST, error del temporizador de intervalos programable	Error del temporizador de intervalos programable
Critical (Crítico)	Error de la POST: Sensor de la POST, error de paridad	Error de paridad
Critical (Crítico)	Error de la POST: Sensor de la POST, falló el SIO	Falla de SIO

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	Error de la POST: Sensor de la POST, falló el controlador de teclado	Fallo de la controladora del teclado
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la inicialización de interrupción de administración del sistema	Falla de inicialización en la interrupción de administración del sistema
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la prueba de apagado del BIOS	Falla de la prueba de apagado del BIOS
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la prueba de apagado del BIOS	Falla de la prueba de la memoria del BIOS durante la POST
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la configuración de Dell Remote Access Controller	Falla de configuración de Dell Remote Access Controller
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la configuración de la CPU	Falla de configuración de la CPU
Critical (Crítico)	Error de la POST: Sensor de la POST, configuración incorrecta de la memoria	Configuración incorrecta de la memoria
Critical (Crítico)	Error de la POST: Sensor de la POST, falló la POST	Error general tras el vídeo
Critical (Crítico)	Error de versión del hardware: Sensor de cambios de versión, se confirmó la incompatibilidad del hardware	Se detectó hardware incompatible
Critical (Crítico)	Error de versión del hardware: Sensor de cambios de versión, se confirmó la incompatibilidad del hardware (firmware del BMC)	El hardware es incompatible con el firmware

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	Error de versión del hardware: Sensor de cambios de versión, se confirmó la incompatibilidad del hardware (no hay correspondencia entre la CPU y el firmware del BMC)	La CPU y el firmware no son compatibles
Critical (Crítico)	Sobrecalentamiento de memoria: Sensor de memoria, se confirmó un ECC corregible <ubicación del DIMM>	Sobrecalentamiento del módulo de memoria
Critical (Crítico)	CRC fatal de SB de memoria: Sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Sur
Critical (Crítico)	CRC fatal de NB de memoria: Sensor de memoria, se confirmó un ECC incorregible	Falló la memoria de puente Norte
Critical (Crítico)	Temporizador de vigilancia: Sensor de vigilancia, se confirmó el reinicio	El temporizador de vigilancia hizo que el sistema se reiniciara
Critical (Crítico)	Temporizador de vigilancia: Sensor de vigilancia, se confirmó la expiración del temporizador	El temporizador de vigilancia expiró pero no se realizó ninguna acción
Aviso	Vínculo de asistencia: Sensor del cambio de la versión, no se declaró un cambio satisfactorio de software ni de firmware	No se pudo actualizar el valor del vínculo de asistencia para lograr un funcionamiento adecuado del NIC
Aviso	Vínculo de asistencia: Sensor del cambio de la versión, no se declaró el cambio de hardware <número de ranura del dispositivo>	No se pudo actualizar el valor del vínculo de asistencia para lograr un funcionamiento adecuado del NIC

Tabla 19-6. Pantalla de estado del servidor *(continuación)*

Gravedad	Message (Mensaje)	Causa
Critical (Crítico)	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró el error de programación de la dirección MAC virtual (n.° de bus, n.° de dispositivo, n.° de función)	No se pudo programar FlexAddress para este dispositivo
Critical (Crítico)	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró el error de la opción ROM del dispositivo para admitir el vínculo de asistencia o Flex Address (tarjeta mezzanine <ubicación>)	La opción ROM no admite ni FlexAddress ni el vínculo de asistencia
Critical (Crítico)	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró el error en obtener datos del vínculo de asistencia o de FlexAddress del BMC/iDRAC6	Falló en obtener información del vínculo de asistencia o de FlexAddress del BMC/iDRAC6
Critical (Crítico)	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró un error de la opción ROM del dispositivo para admitir el vínculo de asistencia o FlexAddress (tarjeta mezzanine XX)	Este suceso se genera si la opción ROM del dispositivo PCI de un NIC no admite el vínculo de asistencia o la función de direccionamiento de FlexAddress
Critical (Crítico)	LinkT/FlexAddr: Sensor del vínculo de asistencia, se declaró un error en la programación de la dirección MAC virtual (<ubicación>)	Este suceso se genera cuando el BIOS no puede programar la dirección MAC virtual en un NIC específico
Critical (Crítico)	Error de E/S fatal: Sensor de grupo de E/S fatal, error fatal de E/S (<ubicación>)	Este suceso se genera en relación con un IERR de CPU e indica cuál de los dispositivos causó el IERR de CPU
Aviso	Error de PCIE no fatal: Sensor de grupo E/S no fatal, error PCIe (<ubicación>)	Este suceso se genera en relación con un IERR de CPU

Visualización del registro del iDRAC6

El **registro** del iDRAC6 es un registro persistente que se mantiene en el firmware del iDRAC6. El registro contiene una lista de las acciones de usuario (como inicio, cierre de sesión y cambios de las políticas de seguridad) y de las alertas generadas por el iDRAC6. El registro se borra al actualizar el firmware del iDRAC6.

El **registro de sucesos del sistema** (SEL) contiene registros de sucesos que ocurren en el servidor administrado, mientras que el **registro** del iDRAC6 contiene registros de sucesos que ocurren en el iDRAC6.

Para acceder al **Registro** del iDRAC6, haga clic en **Sistema→ Configuración de iDRAC→ Registros.** Aparecerá la pantalla **Registro del iDRAC6**. Esta pantalla proporciona la información indicada en la Tabla 19-7.

Tabla 19-7. Información del registro del iDRAC6

Campo	Descripción
Fecha/Hora	La fecha y hora (por ejemplo, `19 dic. 16:55:47`). El iDRAC6 determina la hora a partir del reloj del servidor administrado durante la inicialización del iDRAC6. Si el servidor administrado está apagado al iniciar el iDRAC6, el iDRAC6 obtiene la hora del reloj del CMC del chasis donde reside la tarjeta. **NOTA:** Puesto que el origen de la hora del iDRAC6 es diferente según el estado de la alimentación del servidor administrado (en el momento de la inicialización del iDRAC6), la hora del servidor administrado debe establecerse para que coincida con la hora del CMC. Si la hora del sistema y del CMC no coinciden, se pueden notificar horas incoherentes en los registros del iDRAC6 después de eventos de inicialización del iDRAC.
Origen	La interfaz que ocasionó el suceso.
Descripción	Una breve descripción del suceso y el nombre del usuario que inició sesión en el iDRAC6.

Haga clic en **Borrar registro** para borrar las entradas del registro. El botón **Borrar registro** sólo aparece si tiene permiso para Borrar registros.

Haga clic en **Guardar como** para guardar el Registro de iDRAC6 a un directorio de su elección.

Si al usar Internet Explorer tiene un problema para guardar, asegúrese de descargar la actualización de seguridad acumulada para Internet Explorer que se encuentra en el sitio web de asistencia de Microsoft en **support.microsoft.com**. Si cuando usa Internet Explorer, no puede guardar el Registro del iDRAC utilizando **Guardar como**, puede deberse a la configuración del explorador. Para resolver esto:

1. En Internet Explorer, vaya a **Herramientas→ Opciones de Internet→ Seguridad** y seleccione la zona en la que intenta descargar. Por ejemplo, si el dispositivo iDRAC está en la Intranet local, seleccione **Intranet local** y haga clic en **Nivel personalizado**...
2. En la ventana **Configuración de seguridad**, en **Descargas** compruebe que las siguientes opciones están activadas:
   - Preguntar automáticamente si se debe descargar un archivo
   - Descarga de archivos

PRECAUCIÓN: Para garantizar que el equipo usado para acceder al iDRAC es seguro, en *Varios*, no debe estar activada la opción *Inicialización de aplicaciones y archivos inseguros*.

Visualización de la información del sistema

La pantalla **Resumen del sistema** muestra información sobre los siguientes componentes del sistema:

- Gabinete del sistema principal
- Integrated Dell Remote Access Controller 6: Enterprise

Para acceder a la información del sistema, haga clic en **Sistema→ Propiedades→ Detalles del sistema**.

Ver "Recuperación y solución de problemas del sistema administrado" en la página 377 para obtener información acerca del resumen del sistema, el gabinete del sistema principal y el iDRAC6.

Identificación del servidor administrado en el chasis

El chasis Dell PowerEdge M1000e alberga hasta dieciséis servidores. Para localizar un servidor específico en el chasis, puede usar la interfaz web del iDRAC6 para activar un parpadeo del LED del servidor en color azul. Cuando active el LED, puede especificar el número de segundos que desea que el LED parpadee para asegurarse de que podrá localizar el chasis mientras el LED aún esté parpadeando. Si introduce **0**, el LED parpadeará hasta que usted lo desactive.

Para identificar el servidor:

1. Haga clic en **Sistema→ Configuración del iDRAC→ Solución de problemas**.
2. En la pantalla **Identificar**, seleccione **Identificar servidor**.
3. En el campo **Tiempo de espera para identificar el servidor**, introduzca el número de segundos que desea que el LED parpadee. Introduzca **0** si desea que el LED siga parpadeando hasta que usted lo desactive.
4. Haga clic en **Aplicar**.

El LED del servidor parpadeará en color azul durante el número de segundos que usted haya especificado.

Si introduce **0** para dejar el LED parpadeando, siga estos pasos para desactivarlo:

1. Haga clic en **Sistema→ Configuración del iDRAC→ Solución de problemas**.
2. En la pantalla **Identificar**, deseleccione **Identificar servidor**.
3. Haga clic en **Aplicar**.

Uso de la consola de diagnósticos

El iDRAC6 proporciona un conjunto estándar de herramientas de diagnóstico de red (ver Tabla 19-8) que son similares a las herramientas que se incluyen con los sistemas Microsoft Windows o Linux. Por medio de la interfaz web del iDRAC6, se puede acceder a las herramientas de depuración de red.

Haga clic en **Restablecer iDRAC6** para restablecer el iDRAC. Se realiza una operación de inicio normal en el iDRAC.

Para tener acceso a la pantalla **Consola de diagnósticos**, realice los pasos a continuación:

1. Haga clic en **Sistema→ Configuración de iDRAC→ Solución de problamas**.
2. Seleccione la ficha **Consola de diagnósticos**.

La Tabla 19-8 describe los comandos que se pueden introducir en la pantalla **Consola de diagnósticos**. Introduzca un comando y haga clic en **Enviar**. Los resultados de depuración aparecerán en la pantalla **Consola de diagnósticos**.

Haga clic en el botón **Borrar** para borrar los resultados generados por el comando anterior.

Para actualizar la pantalla **Consola de diagnósticos**, haga clic en **Actualizar**.

Tabla 19-8. Comandos de diagnóstico

Comando	Descripción
arp	Muestra el contenido de la tabla del protocolo para resolución de direcciones (ARP). Las anotaciones del ARP no se pueden agregar ni eliminar.
ifconfig	Muestra el contenido de la tabla de interfaz de red.
netstat	Imprime el contenido de la tabla de enrutamiento.
ping <*dirección IP*>	Verifica que se pueda acceder a la dirección IP de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se debe escribir una dirección IP de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control de Internet) se envía a la dirección IP de destino con base en el contenido de la tabla de enrutamiento actual.
ping6 <*dirección IPv6*>	Verifica que se pueda acceder a la dirección IPv6 de destino desde el iDRAC6 con el contenido actual de la tabla de enrutamiento. Se debe escribir una dirección IPv6 de destino en el campo situado a la derecha de esta opción. Un paquete de eco de ICMP (protocolo de mensajes de control en Internet) se envía a la dirección IPv6 de destino de acuerdo con el contenido de la tabla de enrutamiento actual.
traceroute <*dirección IP*>	Se usa para determinar la ruta que los paquetes toman en una red IP.

Tabla 19-8. Comandos de diagnóstico *(continuación)*

Comando	Descripción
traceroute6 <*dirección IPv6*>	Se usa para determinar la ruta que los paquetes toman en una red IPv6.
gettracelog	Muestra el registro de rastreo del iDRAC6. Para obtener más información, consulte gettracelog en la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) disponible en el sitio web del servicio de asistencia Dell Support en **dell.com/support/manuals**.

Administración de alimentación en un sistema remoto

El iDRAC6 permite realizar de manera remota varias acciones de administración de la alimentación en el servidor administrado. Use la pantalla **Administración de la alimentación** para realizar un apagado ordenado por medio del sistema operativo al reiniciar, encender y apagar el sistema.

NOTA: Debe tener permiso para **Ejecutar comandos de acción de servidor** para realizar acciones de administración de la alimentación. Ver "Cómo agregar y configurar usuarios del iDRAC6" en la página 104 para obtener ayuda con la configuración de permisos de usuario.

1. Haga clic en **Sistema** y luego en **Administración de la alimentación**→ ficha **Control de alimentación**.
2. Seleccione una **Operación de control de alimentación**, por ejemplo, **Restablecer el sistema (reinicio mediante sistema operativo)**. La Tabla 19-9 contiene información acerca de las acciones de control de alimentación.
3. Haga clic en **Aplicar** para realizar la acción seleccionada.

Tabla 19-9. Acciones de control de alimentación

Encender el sistema	Enciende la alimentación del sistema (equivalente a presionar el botón de encendido cuando el sistema está apagado).
Apagar el sistema	Apaga la alimentación del sistema (equivalente a presionar el botón de encendido cuando el sistema encendido).

Tabla 19-9. Acciones de control de alimentación *(continuación)*

NMI (Interrupción no enmascarable)	Envía una interrupción de alto nivel al sistema operativo, lo cual hace que el sistema detenga la operación para permitir actividades fundamentales de diagnóstico o solución de problemas.
Apagado ordenado	Intenta apagar de manera estructurada el sistema operativo y luego apaga el sistema. Requiere un sistema operativo con ACPI (Interfaz de energía y configuración avanzada), lo cual permite que el sistema dirija la administración de la alimentación. **NOTA:** Puede que no sea posible realizar un apagado ordenado del sistema operativo del servidor cuando el software del servidor deja de responder o si no inició sesión como administrador en la consola local de Windows. En estos casos, deberá especificar la ejecución de un reinicio forzado en lugar de un apagado ordenado de Windows. Además, según la versión del sistema operativo Windows, puede existir una política configurada respecto del proceso de apagado que modifique el comportamiento del apagado cuando éste se inicie a partir del iDRAC6. Consulte la documentación de Microsoft que se refiere a la política del equipo local "Apagado: Permitir que el sistema se apague sin tener que iniciar sesión".
Restablecer el sistema (reinicio mediante sistema operativo)	Reinicia el sistema sin apagarlo (reinicio mediante sistema operativo).
Realizar ciclo de encendido del sistema (reinicio mediante suministro de energía)	Apaga el sistema y después lo reinicia (reinicio mediante suministro de energía).

Ver "Supervisión y administración de la alimentación" en la página 321 para obtener más información.

Solución de problemas y preguntas frecuentes

La Tabla 19-10 contiene la preguntas frecuentes sobre cuestiones de solución de problemas.

Tabla 19-10. Preguntas frecuentes/solución de problemas

Pregunta	Respuesta
El indicador LED del servidor parpadea en color ámbar.	Verifique si hay mensajes en el SEL y borre el SEL para detener el parpadeo del indicador LED. Desde Interfaz de la web del iDRAC6, ver "Consulta del registro de sucesos del sistema (SEL)" en la página 381 Desde SM-CLP, ver "Administración de SEL" en la página 340. Desde la Utilidad de configuración del iDRAC6, ver "Menú del registro de sucesos del sistema" en la página 376
Hay un LED de color azul que parpadea en el servidor.	Un usuario ha activado la identificación de localizador del servidor. Ésta es una señal para ayudar a identificar el servidor en el chasis. Ver "Identificación del servidor administrado en el chasis" en la página 398 para obtener información acerca de esta función.
¿Cómo puedo encontrar la dirección IP del iDRAC6?	**En la interfaz web del CMC:** **1** Haga clic en **Chasis→ Servidores** y después haga clic en la ficha **Configuración**. **2** Haga clic en **Deploy** (Implementar). **3** Lea la dirección IP del servidor en la tabla que aparece. **Desde la consola virtual:** • Reinicie al servidor e ingrese a la **utilidad de configuración del iDRAC6** presionando <Ctrl><E>. • Espere la dirección IP que aparece durante la POST del BIOS. • Seleccione la consola "Dell CMC" consola en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos de RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) para obtener una lista completa de los subcomandos RACADM CMC. • Use el comando **getsysinfo** de RACADM local para ver la dirección IP del iDRAC6.

Tabla 19-10. Preguntas frecuentes/solución de problemas *(continuación)*

Pregunta	Respuesta

	Por ejemplo,
	`$ racadm getniccfg -m server-1`
	`DHCP activado = 1`
	`Dirección IP = 192.168.0.1`
	`Máscara de subred = 255.255.255.0`
	`Puerta de enlace = 192.168.0.1`
	En RACADM local:
	Introduzca el comando siguiente en el símbolo del sistema:
	`racadm getsysinfo`
	En la pantalla LCD:
	1 En el menú principal, marque **Servidor** y presione el botón de verificación.
	2 Seleccione el servidor de la dirección IP que busca y presione el botón de verificación.

Tabla 19-10. Preguntas frecuentes/solución de problemas *(continuación)*

Pregunta	Respuesta

¿Cómo puedo encontrar la dirección IP del CMC?	**En la interfaz web del iDRAC6:**
	• Haga clic en **Sistema→ Configuración de iDRAC→ CMC**.
	La dirección IP del CMC se muestra en la pantalla **Resumen** del CMC.
	Desde la consola virtual:
	• Seleccione la consola "Dell CMC" consola en OSCAR para iniciar sesión en el CMC por medio de una conexión serie local. Los comandos de RACADM del CMC se pueden ejecutar a partir de esta conexión. Consulte la *RACADM Command Line Reference Guide for iDRAC and CMC* (Guía de referencia de la línea de comandos RACADM para iDRAC y CMC) para obtener una lista completa de los subcomandos RACADM CMC.
	`$ racadm getniccfg -m chassis`
	`NIC activado = 1`
	`DHCP activado = 1`
	`Dirección IP estática = 192.168.0.120`
	`Máscara de subred estática = 255.255.255.0`
	`Puerta de enlace estática = 192.168.0.1`
	`Dirección IP actual = 10.35.155.151`
	`Máscara de subred actual = 255.255.255.0`
	`Puerta de enlace actual = 10.35.155.1`
	`Velocidad = Negociación automática`
	`Dúplex = Negociación automática`
	La acción anterior también puede realizarse mediante RACADM remoto.

La conexión de red del iDRAC6 no funciona.	• Asegúrese de que el cable de LAN esté conectado al CMC. • Asegúrese de que esté activada en el sistema la configuración de NIC, la de IPv4 o IPv6, y que además esté activada la modalidad estática o DHCP.

Tabla 19-10. Preguntas frecuentes/solución de problemas *(continuación)*

Pregunta	Respuesta
Inserté el servidor en el chasis y presioné el botón de encendido, pero no pasó nada.	• El iDRAC6 requiere un máximo de 2 minutos para inicializarse antes de que el servidor se pueda encender. • Revise el presupuesto de alimentación del CMC. Es posible que el presupuesto de alimentación del chasis se haya excedido.
Olvidé el nombre del usuario administrativo del iDRAC6 y la contraseña.	Deberá restaurar la configuración predeterminada del iDRAC6. **1** Reinicie el servidor y presione <Ctrl><E> cuando se le solicite para ingresar a la **utilidad de configuración del iDRAC6**. **2** En el menú **Utilidad de configuración del iDRAC6**, marque **Restablecer los valores predeterminados** y presione <Intro>. **NOTA:** También puede restablecer el iDRAC6 desde RACADM local ejecutando `racadm racresetcfg`. Para obtener más información, consulte "Restablecer valores predeterminados" en la página 375.
¿Cómo puedo cambiar el nombre de la ranura de mi servidor?	**1** Inicie sesión en la interfaz web del CMC. **2** Abra el árbol **Chasis** y haga clic en **Servidores**. **3** Haga clic en la ficha **Configuración**. **4** Introduzca el nuevo nombre para la ranura en la fila del servidor. **5** Haga clic en **Aplicar**.
Cuando se inicia una sesión de consola virtual en la interfaz web del iDRAC6, aparece una ventana emergente de seguridad de ActiveX.	iDRAC6 puede no ser un sitio de confianza. Para evitar que la ventana emergente de seguridad aparezca cada vez que comience una sesión de consola virtual, agregue el iDRAC6 a la lista de sitios de confianza en el explorador del cliente: **1** Haga clic en **Herramientas→ Opciones de Internet→ Seguridad→ Sitios de confianza**. **2** Haga clic en **Sitios** e introduzca la dirección IP o el nombre DNS del iDRAC6. **3** Haga clic en **Add** (Agregar). **4** Haga clic en **Nivel personalizado**. **5** En la ventana **Configuración de seguridad**, seleccione **Petición** en **Descargar controles ActiveX no firmados**.

Tabla 19-10. Preguntas frecuentes/solución de problemas *(continuación)*

Pregunta	Respuesta
Cuando inicio una sesión de consola virtual, la pantalla del visor está en blanco.	Si usted tiene privilegio de **Medios virtuales**, pero no privilegio de **Consola virtual**, podrá iniciar el visor para acceder a la función de medios virtuales, pero la consola del servidor administrado no aparecerá.
iDRAC6 no responde durante el inicio.	Retire el servidor e insértelo nuevamente. Revise la interfaz web del CMC para ver si el iDRAC6 aparece como un componente que se puede actualizar. Si lo hace, siga las instrucciones de "Actualización del firmware del iDRAC6 por medio del CMC" en la página 131. Si esto no corrige el problema, póngase en contacto con el personal de asistencia técnica.
Cuando trato de iniciar el servidor administrado, el indicador de alimentación es de color verde, pero no hay POST ni vídeo.	Esto puede pasar si se presenta cualquiera de las condiciones siguientes: • La memoria no está instalada o no se puede acceder a ella. • La CPU no está instalada o no se puede tener acceso a ella. • No hay tarjeta de vídeo o no está conectada correctamente. Asimismo, busque mensajes de error en el registro del iDRAC6 desde la interfaz web del iDRAC6 o en la pantalla LCD.

Índice

A

Activación y desactivación de una tarjeta SD, 258

Active Directory
- administración de certificados, 117
- cómo agregar usuarios del DRAC 5, 151
- cómo usarlo con el DRAC 5, 133
- cómo usarlo con el esquema estándar, 160
- cómo usarlo con el esquema extendido, 139
- configuración del acceso al DRAC 5, 143
- extensiones de esquema, 139
- objetos, 140

ActiveX
- complemento de redirección de consola, 236

administración
- almacenamiento, 85

administración de alertas. Consulte *PEF*

administración de almacenamiento de servidor, 85

administración de la alimentación
- cómo usar la interfaz web, 400
- uso de SM-CLP, 340

Agente SNMP, 127

alertas por correo electrónico
- configuración por medio de la interfaz web, 101
- configuración por medio de RACADM, 304

apuntador del mouse
- sincronización, 242

archivo de configuración
- creación, 315

Archivo de imagen, 261

archivo de imagen de inicio
- creación, 352

asistente de redirección de medios, 280, 282

ASR
- configuración, 127
- temporizador de recuperación automática, 87

autentificación de dos factores
- TFA, 189

Autentificación de la tarjeta inteligente, 191

B

bloqueo de IP
  activación, 310
  configuración por medio de la interfaz web, 96
  configuración por medio de RACADM, 308

C

capa de sockets seguros (SSL)
  importación del certificado de firmware, 137

capa de sockets seguros. Consulte *SSL*

Captura de sucesos de plataforma. Consulte *PET*

certificado de servidor
  cómo ver, 117

certificados
  Active Directory, 117
  cómo ver un certificado de servidor, 117
  exportación del certificado CA raíz, 136
  SSL y digitales, 112

Chassis Management Controller. Consulte *CMC*

clave pública, verificar, 58, 60

clave, verificar, 58, 60

CMC
  acerca de, 21
  configuración del iDRAC6 durante la inicialización, 37

códigos de la POST, visualización, 383

comando arp, consola de diagnósticos, 399

comando gettracelog, consola de diagnósticos, 400

comando ifconfig, consola de diagnósticos, 399

comando netstat, consola de diagnósticos, 399

comando ping, consola de diagnósticos, 399

cómo usar RACADM para configurar usuarios del iDRAC6, 107-108

Cómo utilizar el iDRAC6 con el servicio de directorios LDAP, 170

complemento
  instalación de la extensión de Dell, 150

condición del sistema, visualización, 380

conectar o desconectar una partición, 266

conexiones de acceso remoto admitidas, 27

configuración
descripción general de la tarea, 37-41
configuración de los servicios del sistema
Unified Server Configurator, 372
configuración de usuario, 108
configuración de usuarios locales del iDRAC6 para inicio de sesión mediante tarjeta inteligente, 191
configuración de varios iDRAC por medio de RACADM, 319
configuración del inicio de sesión mediante tarjeta inteligente, 189
Configuración e informes en pantalla. Consulte *OSCAR*
consola de diagnósticos, 398
Consulte *RACADM*
contraseña
cambiar, 109
perdida, 375
contraseña administrativa
perdida, 375
CSR
acerca de, 114
generación, 115

D

Descubrimiento automático, 373
documentos que podría necesitar, 29
DRAC 5
configuración, 154, 162

E

eliminar una partición, 268
esquema estándar
cómo usarlo con Active Directory, 160
esquema extendido
cómo usarlo con Active Directory, 139
estación de administración
configuración, 69-79
configuración de la redirección de consola, 231
instalación del software, 83-84
requisitos de red, 69
explorador de web
configuración del servidor proxy, 73
explorador web
admitido, 27
configuración, 70

F

filtración de IP
configuración por medio de RACADM, 306

filtrado de IP
configuración por medio de la interfaz web, 96
Filtro de sucesos de plataforma. Consulte *PEF*
Firefox
acción de las fichas, 92
firma digital, verificar, 57-60
firma, verificar, 57-60
firmware
actualización, 55
actualización por medio de la interfaz web, 129
recuperación con el CMC, 60, 129
Formatear partición, 263
funciones del servidor, integradas
instrumentación, 85
registros, 85

G

Grupo de trabajo de administración distribuida (DMTF), 333
Guía del usuario de Lifecycle Controller, 372

I

iDRAC
actualización del firmware, 55
cómo proteger las comunicaciones, 112
creación de un archivo de configuración, 315
recuperación de firmware, 131
registro, visualización, 396
iDRAC6
configuración del esquema estándar de Active Directory, 171
restablecimiento de los valores predeterminados de fábrica, 375
SSH, 81
iKVM
cómo ver el estado de la consola local, 247
desactivación durante la redirección de consola, 243
iniciar una partición, 269
inicio de sesión mediante tarjeta inteligente, 189
Inicio de sesión único, 185
inicio único, activación, 279
instrumentación
servidor, 85
interfaz web
acceso, 90
actualización del firmware, 129
cierre de sesión, 91
configuración de filtrado de IP, 96
configuración de las alertas de correo electrónico, 101

configuración de las propiedades de LAN de IPMI, 92, 103
configuración de las propiedades de red, 92
configuración de los servicios de iDRAC, 126
configuración de PEF, 100
configuración de PET, 99-100, 303
configuración de SOL, 104
configuración del bloqueo de IP, 96
configuración del explorador, 70
configuración del servicio ASR, 127
configuración del servicio SSH, 127
configuración del servicio Telnet, 127
configuración del servicio Web Server, 126
inicio de sesión, 90
Interfaz web del CMC, 34
interfaz web del CMC
configuración de las propiedades de red del iDRAC6, 42
ubicación de la dirección IP del iDRAC6, 402
interfaz web del iDRAC6, 34, 60
Internet Explorer
configuración, 70
IPMI, 36
configuración con RACADM, 301
configuración de las propiedades de LAN, 92
configuración por medio de la interfaz web, 103
configuración por medio de la utilidad de configuración del iDRAC6, 366
iVMCLI, 35

J

Java
complemento de redirección de consola, 79, 236

K

KVM del iDRAC
visualización de OSCAR, 364

L

lista de dominios de confianza, cómo agregar el iDRAC, 74
localización, configuración del explorador, 75

M

MAP
navegación
medios virtuales
acerca de, 275
configuración por medio de la interfaz web, 278

configuración por medio de la utilidad de configuración del iDRAC6, 370
ejecución, 280
inicio, 282
instalación del sistema operativo, 283
línea de comandos, 355
Mozilla Firefox
desactivación de la lista blanca, 77
versiones admitidas, 77

O

opción de reinicio
desactivación, 87
OpenSSH
cliente SSH para Linux, 81
OSCAR
visualización, 364

P

panel LCD del chasis, 35
pantalla de último bloqueo
captura en el servidor administrado, 86
visualización, 383
Partición vacía, 259
Particiones de vFlash, 253
PEF
configuración por medio de la interfaz web, 100
configuración por medio de RACADM, 303
perfiles de CIM admitidos, 346
permisos de grupo
tabla de, 112
PET
configuración por medio de la interfaz web, 99-100, 303
configuración por medio de RACADM, 303
tabla de sucesos de plataforma que se pueden filtrar, 99
ping6, 399
plataformas
admitidas, 26
Preguntas frecuentes
cómo usar el DRAC 5 con Active Directory, 175
preguntas frecuentes
cómo usar la redirección de consola, 246
uso de los medios virtuales, 284
Propiedades de la tarjeta SD, 255
Propiedades de la tarjeta vFlash SD, 257
propiedades de red
configuración con la utilidad de configuración del iDRAC6, 365
configuración manual, 299
configuración por medio de la interfaz web, 92

configuración por medio de la interfaz web del CMC, 42
configuración por medio de RACADM, 299

Protocolo de línea de comandos de la administración del servidor Consulte *SM-CLP*

Protocolo simple de administración de red. Consulte *SNMP*

Protocolo trivial de transferencia de archivos, consulte *TFTP*

puertos
tabla de, 28

puertos de servicio del iDRAC, 28

Punto de acceso de administrabilidad. Consulte *MAP*

PuTTY, cliente SSH de Windows, 81

R

RACADM
configuración de IPMI, 301
configuración de la filtración de IP, 306
configuración de las alertas por correo electrónico, 304
configuración de las propiedades de red, 299
configuración de PEF, 303
configuración de PET, 303
configuración de SOL, 301
configuración de varios iDRAC, 319
configuración del bloqueo de IP, 308
configuración del servicio SSH, 311
configuración del servicio Telnet, 311
instalación y desinstalación, 78
uso, 289

RACADM local, 35

Recuperación automática del sistema, *Consulte* ASR

redirección de consola
cómo abrir una sesión, 234
configuración, 232
uso, 229

registros
códigos de la POST, 383
iDRAC, 396
servidor, 85

resoluciones de pantalla, compatibilidad, 231

restablecimiento de los valores predeterminados del iDRAC6, 375

reversión del firmware del iDRAC6, 131

S

secuencia de comandos ivmdeploy, 353

secuencias de comandos
ivmdeploy, 353
secure shell. Consulte *SSH*
seguridad, 377
cómo usar los certificados SSL y digitales, 112
SEL
administración por medio de la interfaz web, 381
administración por medio de la utilidad de configuración del iDRAC6, 375-376
servicios
configuración por medio de la interfaz web, 126
servidor
instrumentación, 85
registros, 85
servidor administrado
captura de la pantalla de último bloqueo, 86
configuración, 85
servidor de seguridad, cómo abrir puertos, 28
servidor proxy, configuración del explorador de web, 73
servidor TFTP, instalación, 83
sistema operativo
instalación (método con secuencias de comandos), 351
instalación (método manual), 283
SM-CLP, 36
administración de la alimentación, 340
destinos, 338
formatos de salida, 339
funciones, 335
navegación en MAP
syntax, 335
uso del verbo show, 338
SNMP
prueba de la alerta de captura, 299
SOL
configuración por medio de la interfaz web, 104
configuración por medio de RACADM, 301
Solicitud de firma de certificado. Consulte *CSR*
solución de problemas
indicaciones, 378
SSH
cliente PuTTY para Windows, 81
configuración del servicio de iDRAC por medio de RACADM, 311
configuración del servicio por medio de la interfaz web, 127
instalación de cliente, 80
software OpenSSH para Linux, 81
SSL
acerca de, 113
subcomandos de RACADM
clrraclog, 290

clrsel, 290
config, 87, 290
getconfig, 247, 290, 315
getniccfg, 290
getraclog, 290
getractime, 290
getssninfo, 290
getsvctag, 290
getsysinfo, 291
gettracelog, 291
racreset, 291
racresetcfg, 291
serveraction, 291
setniccfg, 291
sslcertdownload, 292
sslcertupload, 292
sslcertview, 292
sslcsrgen, 292
testemail, 292
testtrap, 292

T

tarjeta SD estándar, 253

Tarjeta vFlash SD, 253

Telnet
configuración de retroceso, 80
configuración del servicio de iDRAC por medio de la interfaz web, 127
instalación de cliente, 80

telnet
configuración del servicio de iDRAC6 por medio de RACADM, 311

tipo de emulación de la unidad flash USB, 370

tipos de sistemas de archivos, 263

traceroute, 399

traceroute6, 400

U

Unified Server Configurator
servicios del sistema, 372

Unified Server Configurator (Configurador de servidor unificado), 372

Update Packages
verificación de la firma digital, 57-60

usuarios
cómo agregarlos y configurarlos por medio de la interfaz web, 104
configuración del usuario de la LAN por medio de la utilidad de configuración del iDRAC6, 372

Utilidad de actualización de DOS, 62

utilidad de configuración del iDRAC
configuración del usuario de la LAN, 372

utilidad de configuración del iDRAC6, 34
configuración de IPMI, 366
configuración de las propiedades de red, 365
configuración de los medios virtuales, 370
inicio, 364
utilidad iVMCLI
acerca de, 351
códigos de retorno, 361
instalación del sistema operativo, 353
opciones de shell del sistema operativo, 361
parámetros, 357
sintaxis, 357
uso, 355
utilidades
dd, 352
iVMCLI, 351
video viewer, 237

V

verificar
clave pública, 58, 60
firma digital, 57-60
video viewer
uso, 237
VLAN, 92

W

web server, iDRAC
configuración por medio de la interfaz web, 126